PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105627

(43)Date of publication of application : 24.04.1998

(51)Int.Cl. G06F 19/00
G06K 17/00
G07D 9/00
G09C 1/00
H04Q 7/38
H04L 9/32

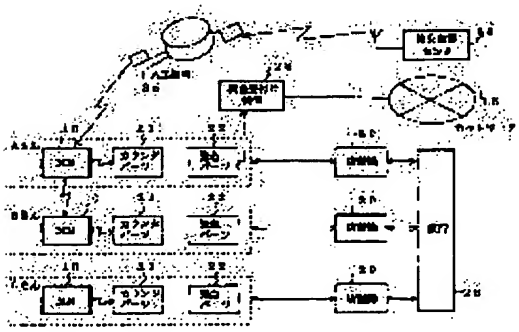
(21)Application number : 08-260009

(22)Date of filing : 30.09.1996

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

(72)Inventor : SAMEJIMA YOSHIKI
KAWASAKI ATSUSHI
YAMADA HIDEO
TAKIMOTO YUICHI

(54) METHOD FOR PROTECTING ELECTRONIC CURRENCY TRANSACTION MACHINE FROM BEING LOST OR STOLEN AND ELECTRONIC CURRENCY TRANSACTION MACHINE



(57)Abstract:

PROBLEM TO BE SOLVED: To protect an electronic currency transaction from being lost or stolen by letting the owner of an electronic currency transaction machine carry equipment, which mutually exchanges an existence confirm signal with a paired electronic currency transaction machine through fine radio waves and issues an caution in the state of stopping receiving the existence confirm signak from the electronic currency transaction machine, with him.

SOLUTION: An electronic money card 10 performs the key transmission of an existence confirm radio wave in respect to an existence confirm inquiry from counter parts 21 paired with that card itself

(1), spontaneously transmits the existence confirm radio wave when the existence confirm inquiry from the counter parts 21 is not dispatched within specified time (2) and spontaneously transmits the existence confirm radio wave when impulse more than a certain degree is received (3). Besides, in case of (2) and (3), the electronic money card 10 temporarily stops a transaction function so as not to transact with the other electronic money card 10. The electronic money card 10 can transmit or stop an SOS while receiving the transmitting instruction or stopping instruction of the SOS from an artificial satellite 25.

JP, 10-105627, A

CLAIMS

[Claim(s)]
[Claim 1]It is a loss theft prevention method of electronic money dealings which trade in electronized currency with one pair of electronic money dealings machines which were published from an accounts machine of a financial institution and stored electronized currency, In the state where sent and received an existence acknowledge signal mutually by a feeble radio wave between electronic money dealings machines used as a pair, and an existence acknowledge signal from an electronic money dealings machine is no longer received. A loss theft prevention method of an electronic money dealings machine which makes an electronic money dealings machine owner carry apparatus which emits warning to an owner of the electronic money dealings machine concerned, and is characterized by preventing loss of electronic money dealings, and a theft.
[Claim 2]An electronic money dealings machine which trades in electronized currency with one pair of electronic money dealings machines which were published from an accounts machine of a financial institution and stored electronized currency, comprising:
When transfer directions to other electronic money dealings machines of electronized currency which self holds through a wireless circuit of the 1st carrier frequency from loss theft rescue plane Seki are received, 1st means to transmit data containing electronized currency to hold on a wireless circuit of the 2nd carrier frequency that enciphers as movement data and is different from directions of said move.
Movement data holding mechanism which holds movement data from other electronic money dealings machines when movement data enciphered from other electronic money dealings machines through a wireless circuit of said 2nd carrier frequency is received.
A transfer processing means to transmit via a network movement data held at this movement data holding mechanism to a predetermined financial institution, and to transfer.
A discarding treatment means to suspend transmission of movement data when a transfer directions stop command is received through a wireless circuit of said 1st carrier frequency from said loss theft rescue plane Seki, and to discard electronized currency which self holds.

[Claim 3]The electronic money dealings machine according to claim 2 transmitting after facing transmitting said movement data on a wireless circuit of the 2nd carrier frequency and making self into dealings disabling.
[Claim 4]The electronic money dealings machine according to claim 2 or 3 having further a means by which self is made into dealings disabling with a predetermined time interval, and an input of a password cancels dealings disabling.
[Claim 5]The electronic money dealings machine according to claim 2 or 3 having further a means to change a password when self is made into dealings disabling with a predetermined time interval.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention is published from the accounts machine of a financial institution, and relates to the loss theft prevention method of an electronic money dealings machine and electronic money dealings machine of

the electronic money trading system which trades in electronized currency with one pair of electronic money dealings machines which stored electronized currency.
It is related with the loss theft prevention method of an electronic money dealings machine and electronic money dealings machine which can collect easily the electronized currency stored by the electronic money dealings machine which discovered easily the electronic money dealings machine which suited loss and a theft especially, or suited loss and a theft, and other data.

[0002]
[Description of the Prior Art]As indicated by the former (the name of an invention; the electronic property data transfer method), for example, JP,8-27815,B, and JP,7-111723,B (the name of an invention; electronic-monetary system), There is art which enabled dealings of a commercial transaction or money loans among individuals or between an individual and non-individuals, such as a store, with the data carrier (electronic money dealings machine) or dealings module which stored the electronized currency (electronic money) equivalent to currency.
[0003]
[Problem(s) to be Solved by the Invention]However, if it was in the art indicated by the above-mentioned gazette, there was a problem that consideration was paid to neither loss of an electronic money dealings machine nor recovery of the electronic money dealings machine to a theft or its receiving data.
[0004]Made in order that this invention may solve the above-mentioned problem, the 1st purpose is to provide the loss theft prevention method of the electronic money dealings machine which can prevent loss by mislaying after the fall from the body of an electronic money dealings machine, or use.
[0005]The 2nd purpose is to provide the electronic money dealings machine which can collect easily the electronized currency stored by the electronic money dealings machine or electronic money dealings machine which suited loss and a theft, and other data.
[0006]Whenever the 3rd purpose of this invention goes through a prescribed period so that the safety of an electronic money dealings machine can be improved, it suspends the function of an electronic money dealings machine, It is in providing the electronic money dealings machine of which the stall of an electronic money dealings machine can be canceled by the input of the password changed for between [every] homonomy scheduled time.
[0007]
[Means for Solving the Problem]In order to attain the 1st purpose of the above, a loss theft prevention method of an electronic money dealings machine of this invention, In the state where sent and received an existence acknowledge signal mutually by a feeble radio wave between electronic money dealings machines used as a pair, and an existence acknowledge signal from an electronic money dealings machine is no longer received. An electronic money dealings machine owner is made to carry apparatus which emits warning to an owner of the electronic money dealings machine concerned, and loss of electronic money dealings and a theft are prevented.
[0008]In order to attain the 2nd purpose, an electronic money dealings machine of this invention is provided with the following.
When transfer directions to other electronic money dealings machines of electronized currency which self holds through a wireless circuit of the 1st carrier frequency from loss theft rescue plane Seki are received, 1st means to transmit data containing electronized currency to hold on a wireless circuit of the 2nd carrier frequency that enciphers as movement data and is different from directions of said move.
Movement data holding mechanism which holds movement data from other electronic money dealings machines when movement data enciphered from other electronic money dealings machines through a wireless circuit of said 2nd carrier frequency is received.
A transfer processing means to transmit via a network movement data held at this movement data holding mechanism to a predetermined financial institution, and to transfer, A discarding treatment means to suspend transmission of movement data when a transfer directions stop command is received through a wireless circuit of said 1st carrier frequency from said loss theft rescue plane Seki, and to discard electronized currency which self holds.

[0009]It faces transmitting movement data on a wireless circuit of the 2nd carrier frequency, and it is made to transmit here after making self into dealings disabling.

[0010]In order to attain the purpose of **** 3, an electronic money dealings machine of this invention, A password was changed, when self was made into dealings disabling with a predetermined time interval, an input of a password canceled dealings disabling and self was further made into dealings disabling with a predetermined time interval.
[0011]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail with reference to drawings.
[0012]It is enciphered that especially the data transmitted and received between the apparatus in an embodiment of the invention is decipherable only between transceiver subject equipment unless it refuses. Publicly known encoding technology is used for this encryption.
[0013]The electronic money dealings machine (= MM and the following call it an electronic money card) 10, and 11a-11c which drawing 1 is a system configuration figure showing the embodiment of the electronic money trading system which applied this invention, and were published from the accounts machine of the bank A, The electronic money card 12 published from the accounts machine of the bank B exists. The dashed line in drawing 1 specifies a relation with an issuing bank.
[0014]Among these, although the electronic money cards 10 and 12 are independent electronic money cards without child-parent relationship, in the accounts machine of the bank A, as for the electronic money cards 11a-11c, the child-parent relationship of parents, a child, and a grandchild is set up.
[0015]Any electronic money cards 10, 11a-11c, and 12 are constituted so that a cellular phone is possible, Dealings of electronized currency EMs are attained among POS terminals 13 and 14 which can trade in the accounts machine of a bank, other electronic money cards, the electronic money cards of child-parent relationship, or electronized currency EM. It is connected in the network 15, and through this network 15, the banks A and B are constituted so that dealings of inter-bank electronized currency EMs may be possible.
[0016]However, about the electronic money cards 11b and 11c which have parents as their own higher rank machine, dealings are restricted with the attribute set up by parents. The low rank machine cannot delete freely the attribute set up from the higher rank machine. However, the attribute added by itself can be deleted freely. [of the attribute] [an addition and oneself]
[0017]It is enciphered according to the encryption algorithm using the publicly known account art of a symmetrical key signal book, and electronized currency EM dealt with transfers to business contacts.
[0018]The electronic money cards 10, 11a-11c, and 12 in which these cellular phones are possible are faced being published from the accounts machine of a bank, and identification information (ID) is set [that it is an individual's possession and] up.
[0019]POS terminals 13 and 14 are also published from the accounts machine of the banks A and B, and identification information (ID) is set [that it is a non-individual's possession and] up on the occasion of the issue.
[0020]When trading in electronized currency EM, as the solid line S shows, a session (channel) is established between partner machines. This session (channel) is established by the means using known art, such as direct continuation by a cable etc., light, a feeble radio wave, and inductive coupling.
[0021]In order that the electronic money cards 10, 11a-11c, and 12 may support the dealings based on budget planning, have the currency holder according to budget cost item, but. The communications program with a personal computer is built in so that it can set up arbitrarily with the external personal computers 16, 17, and 18 about the structure of this currency holder. Standard folder structure is prepared, either of these is chosen, and it is corrected and used at the beginning if needed.
[0022]The electronic money cards 10, 11a-11c, and 12, As shown in drawing 2 on behalf of the electronic money card 11a, it has the connection interface 110 with the personal computer 17, the connection interface 111 with other electronic money cards 12, and the connection interface 112 with POS terminal 19, Furthermore, the balance, transaction money amount, etc. of electronized currency EM in a currency holder. The operation-sides side is equipped with the letter-key part 122 which comprises a key and the cursor control keys 121, such as the indicator 114 to display, the function key part 115 which pays and comprises the manual operation button of the key 116, the balance introduction key 117, the acceptance key 118, the cancellation key 119, and signature-keys 120 grade, a number, and an alphabetic character.
[0023]The payment key 116 is a key operated when a transaction content with a partner agrees and a partner

machine is made to actually transfer electronized currency EM. When trading between POS terminals 19, it can constitute instead of [this] paying and operating the key 116 so that the "disbursement approval key" installed in POS terminal 19 may be operated.

[0024]The balance introduction key 117 is for displaying the balance of electronized currency EM in a currency holder, and whenever it operates this balance introduction key 117, the balance of the following currency holder is displayed.

[0025]The acceptance key 118 is a key operated when accepting electronized currency EM from a partner machine.

[0026]The cancellation key 119 is a key operated when canceling dealings, and if this cancellation key 119 is operated, the session established between partner machines will be cut.

[0027]The signature keys 120 are keys operated when transmitting the signature of the transfer origin of electronized currency EM to a partner machine, and are used at the time of dealings of checks etc.

[0028]Although the connection interface 110,111 with the personal computer 17 and other electronic money cards 12 shows the connected example by a cable and the connection interface 11 with POS terminal 19 shows the example connected by the feeble radio wave in drawing 2, It is not limited to this.

[0029]However, the connection interface 112 with POS terminal 19 has it, when the one connected by the feeble radio wave faces trading in electronized currency EM among many and unspecified customers and advances processing efficiently. [effective]

[0030]If drawing 3 is a functional block diagram showing the internal function of the electronic money cards 10, 11a-11c, and 12 and it divides roughly, The memory 130, CPU135, the clock/timer 136, the input/output interface 137, the keyboard interface 138 with each operation key of operation sides, the indicator interface 139, the interface 140 with an external personal computer, Transmission and reception with the transmitter-receiver 144 for performing the interface 141 with other electronic money cards, the interface 142 with a POS terminal, and communication with an artificial satellite, the transmitter-receiver 143 for performing transmission and reception with other electronic money cards, and the counter part mentioned later. It has GPS receiver 146 for performing position recognition by the transmitter-receiver 145 for carrying out, and GPS (position recognition system using an artificial satellite).

[0031]And in the memory 130. Electronized currency EM (electronic money). Substitution money to store, such as the safe 1301 and a coupon. The substitution money hangar 1302 and transaction history to store. The transaction log hangar 1303 to store, the money holder 1304 which stores the amount of money of purpose-for-spending purpose-oriented electronized currency EM, the storage area 1305 which stores issuing bank ID, the storage area 1306 which stores self-opportunity ID, the storage area 1307 which stores higher rank machine ID, and low rank machine ID. In order to restrict the purpose for spending of the storage area 1308 to store and electronized currency EM. The attribute of the self-opportunity to be used. The transcriptional region 1313 for sending and receiving the data transmitting between the storage area 1309 to store, a personal computer communication pro's storing region 1310, the storing region 1311 of the program for dealings machines, and these storing regions 1310 and 1311, the storing region 1312 of a code/decoding program, The data transmitted and received by the transceiver program 1315 with the counter part mentioned later, the communications program 1316 with an artificial satellite, the transceiver programs 1317 between other electronic money cards, and these programs 1315-1316 and 1317. The transmitted-and-received-data holding area 1318 to hold is formed.

[0032]Drawing 4 is an explanatory view showing roughly the processing of the dealings inside of a plane in the case of making payment for a purchasing commodity by electronized currency EM between the electronic money card 11b and POS13, and the flow of electronized currency EM. In drawing 4, the electronic money card is the same as a retail business machine.

[0033]The person having of the electronic money card 11b purchases goods at the store in which POS13 was installed, When it is going to pay by electronized currency EM in the electronic money card 11b and you are going to make it complete dealings, the person having of the electronic money card 11b makes the electronic money card 11b approach the reader of POS13, and establishes the session of the electronic money card 11b and POS13 by a feeble radio wave.

[0034]If commodity attributes read by the bar code reader of POS13, such as the amount billed about a purchasing commodity and a merchandise name, and a class of goods, have been sent from POS13 in this state, The electronic money card 11b investigates whether the money holder according to use item corresponding to a class of goods (purpose-for-spending purpose-oriented) exists, Even if it case or exists, when [not existing] the amount of money for maintenance is less than the amount billed, it judges with dealings being impossible and payment of electronized

currency EM is made disapproval (Step 1701).
[0035]However, when the money holder according to use item corresponding to a class of goods (purpose-for-spending purpose-oriented) exists and the amount of money for maintenance exceeds the amount billed next, a use restriction check is performed (Step 1702).
[0036]Prohibition/release of the payment from the accounts machine of the bank set as the storage area 1309 of a self-opportunity attribute in detail, The number of times of an electronic money transfer limit per day, the limit per 1-time dealings, the amount of a trading limit per day, When attribution information, such as information periods (end of the month etc.) to a higher rank machine, low rank machine person having's date of birth, and ID of a report higher rank machine, is taken out, this attribution information and class of goods, a merchandise name, the amount billed, etc. are compared and it corresponds to a dealings inhibition condition, payment of electronized currency EM is made disapproval (Step 1702).
[0037]The case where it corresponds to a dealings inhibition condition refers to the case where minors try to purchase tobacco, for example, and a message to that effect and applicable merchandise name are displayed on the indicator 114.
[0038]However, when it does not correspond to a dealings inhibition condition, it pays, the button 116 is operated, the payment of electronized currency EM is permitted on the conditions as which the buyer's purchase volition was determined, electronized currency EM of the amount billed is pulled out from the safe 1301, this is enciphered, and it transmits to POS13.
[0039]POS13 which received electronized currency EM transmits a receipt and its ID to the electronic money card 11b, when the payment of electronized currency EM is received and the issue requesting of a receipt occurs. When the payment of electronized currency EM is received and the message of the purport that a coupon is used is received, the amount of money of a coupon is deducted from the amount billed, and let the remainder be the amount billed. And by this new merchandise purchase, a coupon is published, it transmits to the electronic money card 11b, and a session is cut.
[0040]After session cutting, the electronic money card 11b stores in the storage area 1303 of a transaction log the transaction history containing a receipt, and ends processing of transactions.
[0041]Whether whether a coupon's being used and or not a receipt are required sets up beforehand, before purchasing goods. This is set up by the key operation of the letter-key part 122.
[0042]Drawing 5 is a system configuration figure showing the composition of the principal part of a loss theft preventive function in the electronic money trading system which applied this invention, and drawing 1 and identical parts are expressed with the same sign. In the following composition, it is enciphered that especially the data transmitted and received between apparatus is decipherable only between transceiver subject equipment unless it refuses. Publicly known encoding technology is used for this encryption.
[0043]In drawing 5, 10 is an electronic money card in which electronic money etc. are stored. 21 is a counter part which accomplishes the electronic money card 10 and a couple and prevents the loss theft of the electronic money card 10. 22 is an urgent part of the electronic money card 10, and the telephone number of the receiver's address when the electronic money card 10 carries out a loss theft is memorized.
[0044]An urgent accepting device with which 23 carries out the loss robbery report and electronic money recovery report of the electronic money card 1, The loss theft center in which 24 receives a ****** robbery report and an electronic money recovery report, The artificial satellite with which 25 performs the various directions from the loss theft center 24 to the electronic money card 10 made into the referent, each financial institution where 26 published the electronic money card 10, and 20 are store machines currently installed in a financial institution, a public facility, etc.
[0045]Below, the functional outline of each device is explained individually.
[0046](1) The electronic money card 10 electronic money card 10 is provided with the following function for [other than the electronic money transaction function mentioned above] loss theft prevention.
[0047]An existence check electric wave is sent to the existence check inquiry from the counter part 21 which accomplishes the <dispatch of existence check electric wave for loss theft prevention> ** itself, and a pair.
[0048]** If the existence check inquiry from the counter part 21 does not arrive in a prescribed period, an existence check electric wave will be sent spontaneously.

[0049]** If the above shock is got to some extent, an existence check electric wave will be sent spontaneously.
[0050]In the aforementioned ** and **, the electronic money card 10 suspends a dealings function temporarily so that dealings with other electronic money cards 10 cannot be performed.
[0051]Dispatch of SOS at the time of a loss theft and the <stop> electronic money card 10 can send SOS in response to dispatch directions or stop instruction of SOS from the artificial satellite 25, or it can be stopped.
[0052]With other electronic money cards 10, in order to collect electronic money from the electronic money card 10 with a loss theft, in the data of SOS, the electronic money which the electronic money card 10 which sent SOS holds is enciphered, and it exists so that this electronic money (EM) cannot be used.
[0053]A dealings function is suspended so that dealings with other electronic money cards 1 cannot be performed, when SOS is sent.
[0054]When stopping SOS, the held electronic money is discarded.
[0055]The <received of SOS> electronic money card 10 can receive SOS which other electronic money cards 10 sent.
[0056]The electronic money card 10 which received SOS incorporates SOS into the self-electronic money card 10, and tells at a suitable stage "Since SOS is held, a report is required" by vibration / sound / blink to the carrier of the self-electronic money card 1. If this is not sent within a period with the carrier of the electronic money card 10 which received SOS, the electronic money card 10 which received SOS may suspend an own function. Whether it is made to stop or it is not made to stop can set up a financial institution with the owner's degree of bank credit.
[0057]The enciphered photograph of the person himself/herself is stored in the electronic money card 10, and substitution is impossible.
[0058]The output of the electric wave which the <strength of electric wave> electronic money card 10 transmits to the counter part 21 is larger than the existence check inquiry electric wave which the counter part 22 sends.
[0059](2) The counter part 21 <purpose of counter part 21> counter part 21 is for loss early detection of the electronic money card 10, and accomplishes the electronic money card 10 and a couple. The electronic money card 10 detects the regulation distance from the body of a carrier, or that the prescribed period separated, and tells a carrier about it.
[0060]Usually, usual states, such as accessories / wrist watch / glasses / belt buckle, are equipped at the body of a carrier, and the thing to carry.
[0061]Drawing 6 is a functional block diagram showing the composition of the counter part 21, The interface 213 with CPU210, the dealings machine deferred receiving agent 211 with other electronic money cards stored in the memory, the liquid crystal display (LCD) 212, and the buzzer 214, the transmitter-receiver 216 with the electronic money card 10 which accomplishes a pair, an interface with this transmitter-receiver 216, It has the metal fittings 218 for fixing to some of antennas 217, dresses, or personal effects, and the search button 219.
[0062]The <neighborhood existence acknowledgement function> counter part 21 performs the existence check inquiry by an electric wave to the electronic money card 10 corresponding at intervals of a prescribed period. The electronic money card 10 which received the inquiry answers an above-mentioned self-card's existence check. When the response from the electronic money card 10 is not able to be received in a prescribed period, vibration / sound / blink carries out counter part 21 self, and the carrier of the counter part 21 is told about that.
[0063]Also when the existence check which the electronic money card 10 sent spontaneously is received, vibration / sound / blink carries out counter part 21 self, and the carrier of the counter part 21 is told about that.
[0064]The <halt of neighborhood existence acknowledgement function> carrier will be able to stop an existence acknowledgement function temporarily soon. In this case, the counter part 21 connects that to the electronic money card 10 which accomplishes itself and a pair.
[0065]The carrier of the <gestalt> electronic money card 10 is usually carrying the counter part 21 with the electronic money card 10. The counter part 21 is carried by the body so that it may usually be hard to separate from the body. Carrying of the gestalt which the counter part 21 included beforehand in accessories, such as a necklace, a ring, a bracelet, a nose ring, glasses, and a belt buckle, is also considered.
[0066]In this case, a functional rise can be carried out so that the direction/distance data received by the existence check received from the electronic money card 10 may be displayed. The individual which controls vibration / sound / blink by intensity of a reception radio wave is made, so that the electronic money card 10 is approached.
[0067]Since loss of counter part 21 self is also considered, it is desirable to carry two or more pieces to a person every electronic money card 10.

[0068](3) The purpose / urgent part 22 <functional> urgent part 22 is the telephone cards for reports to the loss theft of the electronic money card 10.
[0069]The telephone number of the loss theft center 24 which are one or more electronic money card ID and receiver's addresses is set up. The loss theft of the electronic money card 10 can be sent to the loss theft center 24 by inserting the urgent part 22 in the urgent accepting device 23 or telephone.
[0070]Since the urgent part 22 is cheap, it is desirable to hold about ten sheets and to make every place dotted with the urgent part 22 of an identical content to all the electronic money cards 10 which the one electronic money card 10 or a family holds.
[0071]By this scattering, even if the electronic money card 10 and the counter part 21 are taken by sneak-thieving / burglar / threat together with this urgent part 22, it can leave somewhere the urgent part 22 which was not taken.
[0072]When the loss theft of the electronic money card 10 is suited, in order to make it sent immediately, walking around with the urgent part 22 is desirable.
[0073](4) The urgent accepting device 23 <purpose> urgent accepting device 23 is a device for sending the electronic money card 10 which suited the loss theft to the loss theft center 24. It is also a device for sending SOS which received from the electronic money card 10 which suited the loss theft to the loss theft center 24.
[0074]If the <functional> urgent part 22 is inserted in the urgent accepting device 23, the urgent accepting device 23 will display 1 or two or more electronic money card ID which are registered into the inserted urgent part 22 on the indicator of the urgent accepting device 23. And electronic money card ID with the selected person who inserted the urgent part 22 is sent to the loss theft center 24 as electronic money card ID of the electronic money card 10 used as a loss theft.
[0075]The <setting position> urgent accepting device 23 is installed in this branch office of a financial institution, a post office, a police station police box, a station, a hospital, a public facility, etc.
[0076](5) The loss theft center 24 <purpose> loss theft center 24 is a control center of the electronic money card 10 which suited the loss theft.
[0077]That is connected to the financial institution 26 which pointed to the <functional> loss theft center 24 to the artificial satellite 25 so that SOS might be made to send from the urgent accepting device 23 to the electronic money card 10 of electronic money card ID with a notification, and published the electronic money card 10 concerned.
[0078]When the electronic money which the electronic money card 10 which suited the loss theft held is collected, that is connected to the financial institution 26 which pointed to the artificial satellite 25 so that the electronic money card 10 might be made to stop dispatch of SOS, and published the electronic money card 10 concerned.
[0079](6) The artificial satellite 25 <purpose> artificial satellite 25 is repeating installation which transmits the directions from the loss theft center 24 to the electronic money card 10.
[0080]The <functional> artificial satellite 25 carries out dispatch of SOS, or directions of a stop to the electronic money card 10 of electronic money card ID directed from the urgent accepting device 23.
[0081]Below, the outline of a loss theft preventive function is explained.
[0082]First, loss theft prevention is explained.
[0083](1) The case 1 <usual> counter part 22 is always performed with the time interval of regulation of an inquiry of the existence check shown in drawing 9 to the electronic money card 10. The electronic money card 10 performs the existence Acknowledgement shown in drawing 10 to the counter part 21 to this inquiry. Therefore, it can check that the partner exists mutually near the self-opportunity in the range which the electric wave which each sends reaches.
[0084](2) While the carrier of the case 2 <case [by fall of the electronic money card 10, the size of the shock is beyond regulation]> electronic money card 10 walks, the electronic money card 10 is dropped, When the dropping impact which the electronic money card 10 received is beyond regulation, electronic money card 10 self sends spontaneously the data of the existence check spontaneous dispatch shown in drawing 12.
[0085]When this data is received, vibration / sound / blink carries out counter part 21 self, and it warns the electronic money card 10 carrier concerned of the counter part 21. The carrier which is continuing walking without this noticing that it dropped can notice that it dropped the electronic money card 10 immediately, and can escape loss by fall etc.
[0086](3) The case 3< dropping impact is monitoring continuously whether below regulation >** electronic money card 10 self has the existence check inquiry from the counter part 21 in a prescribed period. Therefore, after the existence check inquiry sent from the counter part 21 stopped reaching the electronic money card 10, if it goes

through this prescribed period, the data of existence check spontaneous dispatch will be sent from the electronic money card 10. In the radio wave output of the existence check spontaneous dispatch which the electronic money card 10 sends, since the output is larger than the output of the existence check inquiry electric wave from the counter part 21, the counter part 21 will receive the data of existence check spontaneous dispatch in this case. By this reception, vibration / sound / blink carries out counter part 21 self, and it warns the electronic money card 10 of the counter part 21.

[0087]** The counter part 21 is measuring the distance of the counter part 21 and the electronic money card 10 with the intensity (receiving field intensity) of the electric wave of the received existence Acknowledgement. When this measured distance becomes larger than regulation distance, vibration / sound / blink carries out counter part 21 self, and it warns electronic money card 10 carrier of the counter part 21. Vibration / sound / blink is strengthened, so that the counter part 21 displays it based on the direction/distance data sent out from the electronic money card 10 and approaches the electronic money card 10.

[0088](4) Since ** distance <an existence check inquiry reaches the electronic money card 10 although forgotten> is measured, it is the same as the case where it is ** of "a dropping impact is below regulation". [case 4]

[0089](5) the case 5 <although an existence check inquiry does not arrive, the existence check spontaneous dispatch from the electronic money card 10 reaches the counter part 2> -- a case 3< dropping impact is the same as below regulation > in this case.

[0090](6) the case 6 <the existence check spontaneous dispatch from the electronic money card 10 does not reach the counter part 21> -- the carrier of the electronic money card 10 will look for an idea for the counter part 2 to reliance in this case.

[0091]When the counter part 21 receives the existence check spontaneous dispatch which the electronic money card 10 sends by carrying out the depression of the search button 219 of the counter part 21, Vibration / sound / blink can be strengthened, so that the counter part 21 displays it based on the direction/distance data sent out from the electronic money card 10 and approaches the electronic money card 10.

[0092](7) Case 7 <loss> Even if searched, when it is not found or the warning of the counter part 21 is not noticed (i.e., when it loses), it will send to the loss theft center 24 using the urgent part 22.

[0093](8) Case 8 <theft> It is the same as the case 7 "loss" in this case.

[0094]Below, operation of the system about the case of the case 7 "loss" and the case 8 "theft" is explained. Operation of the system in these cases is the same.

[0095]When the loss theft of the electronic money card 10 is suited, the carrier of the electronic money card 10 uses the urgent part 22. 1 or electronic money card ID of two or more electronic money cards 10, the telephone number of the loss theft center 24, etc. are beforehand set to the urgent part 22. This is inserted in the urgent part 22 inserted slot of nearby telephone or the urgent accepting device 23. When the urgent part 22 is inserted in telephone, the telephone displays 1 or two or more electronic money card ID which are registered into the inserted urgent part 22 on the indicator of telephone. The person who inserted the urgent part 22 in telephone chooses electronic money card ID of the electronic money card 10 which suited the loss theft from displayed electronic money card ID. Selected electronic money card ID turns into electronic money card ID of the electronic money card 10 with a loss theft, and is sent out automatically to the loss theft center 24.

[0096]The urgent part 22 can also be inserted in the urgent accepting device 23. Operation of the urgent accepting device 23 in this case is the same as operation of telephone.

[0097]When there is only one electronic money card ID registered into the urgent part 22, this electronic money card ID turns into electronic money card ID of the electronic money card 10 with a loss theft.

[0098]The telephone or the urgent accepting device 23 with which the urgent part 22 was inserted transmits electronic money card ID which was carried out in this way and determined to the loss theft center 24.

[0099]The urgent accepting device 23 is installed in this branch office of a financial institution, a post office, a police station, the police box, the station, the hospital, the public facility, etc.

[0100]The loss theft center 24 which received electronic money card ID from the urgent accepting device 23 transmits electronic money card ID to the artificial satellite 25 while registering electronic money card ID which received into a loss theft database.

[0101]The artificial satellite 25 specifies the electronic money card 10 which carries out the carrier of electronic

money card ID transmitted from the loss theft center 24, and has electronic money card ID which received as the SOS dispatch electronic money card 10, and broadcasts SOS dispatch directions.

[0102]The electronic money card 10 which received this SOS broadcasting from the artificial satellite 25 disregards this broadcasting, when electronic money card ID broadcast is not electronic money card ID of the self-electronic money card 10.

[0103]However, when electronic money card ID broadcast is electronic money card ID of the self-electronic money card 10 (let this electronic money card 10 be the card S henceforth), the card S performs an own dealings stall. And the balloon of the built-in which has led to the card S with the vinyl tube etc. is emitted outside, and built-in gas is poured in and swollen. By this, if the card S is not caught in something, it will appear all over water sky, and it will broadcast from the air.

[0104]SOS is broadcast, even when the card S is caught in something and cannot float all over water sky. Broadcasting of SOS is performed to the following apparatus.

[0105]a. Electronic money card 10 (henceforth) with electronic money card ID of the card S, and electronic money card ID which has a specific relation it is considered as the card R -- 1 which received SOS from the b. urgent accepting device 23c. loss theft center 24 card S, or two or more above-mentioned apparatus receive SOS broadcast from the card S, and incorporate the SOS into self-apparatus.

[0106]Operation of the electronic money card 10 (card R) which incorporated SOS into below is explained.

[0107]The card R calculates "what day back" from the information period which tells the carrier of the card R about the purport of SOS reception by electronic money card ID of the card R, for example, an SOS receiving day. And if the report date of SOS reception comes, the carrier of the card R will be told about the purport of SOS reception by vibration / sound / blink.

[0108]The carrier of the card R which got to know this by making the urgent accepting device 23 and the card R which are installed in nearby telephone or a financial institution book branch office, a post office, a police station, a police box, a station, a hospital, a public facility, etc. within the constant period from a report date communicate, SOS which the card R holds is transmitted to the loss theft center 24 by urgent accepting device 23 course.

[0109]The loss theft center 24 gets to know electronic money card ID of the electronic money card 10 (card S) which had the loss theft from SOS collected by the urgent accepting device 23 course, and investigates the solution database which holds whether the incident of this card S is solved in the self-center 24. If it does not register with a solution database as a result of investigation, the contents of registration of a solution database will be erased noting that an incident is solved.

[0110]Next, the loss theft center 24 transmits electronic money card ID of the card S to the artificial satellite 25 so that it may stop broadcasting of SOS of the card S.

[0111]Next, the loss theft center 24 transmits SOS of the card S to the financial institution 26 which published the card S. The financial institution 26 which received transmission of SOS informs that it collected the electronic money of the card S, etc. from electronic money card ID of the card S to the change nominee with the nominee who registered when issue of the card S was received, or a subsequent report. Though natural, when the card S broadcasts SOS to collected SOS, all electronic money of the amount of money and other data that the card S held are contained.

[0112]The artificial satellite 25 broadcasts SOS stop instruction to the card S directed from the loss theft center 24. The apparatus which receives broadcasting of SOS stop instruction and carries out a certain operation is the card S and the card R.

[0113]The card S will stop broadcasting of SOS, if this stop instruction is received, and it separates a balloon. Existence check spontaneous dispatch is performed.

[0114]About the card R, when it is the card R holding SOS in which the card R has electronic money card ID of the card S, SOS with electronic money card ID of the card S is discarded. Therefore, in the card R which received SOS from the card S, also when discarding SOS before a report to the carrier of the self-card R, while the carrier of the card R does not know at all for a certain reason, the card R which he holds may have received and discarded SOS.

[0115]The store machine 20 in which it trades with the electronic money card 10 which an individual holds, When the electronic money card 10 of the individual maintenance which is business contacts is the card R holding SOS data, Even if it is before an SOS maintenance report to the carrier of the card R, the card R has a function which incorporates SOS of two or more cards S currently held from the electronic money card 10, and can transmit

incorporated SOS to the loss theft center 24. That is, the store machine 20 also has the vicarious execution function of the urgent accepting device 23.

[0116]The electronic money card 10 which it did [electronic money card] in this way and had SOS incorporated discards all the SOS which self holds.

[0117]Next, the measure about prevention of use of those who are not just carriers of the electronic money card 10 is explained with reference to drawing 7 and drawing 8.

[0118]As shown in <24h effective password> drawing 7, a required number user sets up the password of truth mixing as a password. Here, Pt1-Ptn are true passwords, and Pf1-Pfm are fake passwords.

[0119]The method of password setting out here also needs fake password input intentionally rather than enters only a true password. And a password differs in the true number of passwords and the fake number of passwords to input by the difference in a day of the week, or the difference in a date.

[0120]This method is explained using drawing 7. If a password is not entered before use of the beginning on the day, the electronic money card 10 is in a temporary stall state. First, in the input of a password, all the passwords of truth mixing registered into the electronic money card 10 concerned are displayed on the electronic money card 10 concerned at a built-in display. The carrier of the electronic money card 10 concerned chooses the password entered as follows from the password of displayed truth mixing. A question which it tells a password "is next ?" in the input by selection of a password whenever the one electronic money card 10 is chosen is still no action, without carrying out. namely, the input of a password is an end now -- or whether a password is entered succeedingly entrusts the input person of a password. And if the entered password differs from the password on the day as a result of declaration of the end of password input, a "password error" will only be displayed. When this "password error" reaches the regular number of times continuously, use of regular days is suspended.

[0121]Next, the method of the concrete input of a password is described. When that day is Sunday, a password is entered before use of the beginning of this day, but the number of the passwords of imitations with true as arbitrary passwords with an arbitrary password entered since it is Sunday as one piece is three. This becomes usable [the electronic money card 10 in that day] on Sunday. And this password expects 0:00 a.m. on the next day, and becomes invalid. That is, anew, if the password of two pieces and arbitrary imitations is not entered two pieces, on Monday of the next day, use of the electronic money card 10 becomes impossible [arbitrary true passwords] from 0:00 a.m. on Monday of the next day.

[0122]Also in drawing 8, it is the same. The difference between drawing 7 and drawing 8 is only a difference in whether a password is changed by a day of the week, or it changes by a date.

[0123]Since a possibility of choosing a true password one piece like the input method of other passwords is high even if the person who stole the electronic money card 10 investigates the attribute of a just carrier and guesses a password by this, Use of those who are not just carriers of the electronic money card 10 can be prevented with high probability.

[0124]That the electronic money card 10 which the theft person stole without the input of a password can be used, It is only a case where the stall directions from the artificial satellite 25 to the electronic money card 10 where the electronic money card 10 was stolen with the counter part 21 and which had the theft are not of use for use of the theft person of theft that day. And it is only theft that day.

[0125]The electronic money card 10 can set up the limit of the amount of money which can be used on the 1st as a preset value, and can also increase this temporarily. Even when the operating limit on the 1st is increased, after regular time progress returns to the original preset value.

[0126]Therefore, the damage amount of money by a theft can be further lessened by using two kinds of password methods, the password method for functional activation of the electronic money card 10, and the password method for the operating limit increase on the 1st.

[0127]If the attributes (for example, a birthday, a telephone number, a room number, etc.) of the person himself/herself are included in a password, a password will be able to be presumed by investigating the person of the person himself/herself. Then, by including the attribute of a cardholder's lie intentionally in a password, presumption of a password can become difficult and can raise an unauthorized use preventive effect further.

[0128]Drawing 9 is a data content of the existence check inquiry 40 which transmits to the electronic money card 10 from the counter part 21, asks electronic money card ID41 and consists of the code 42.

[0129]Electronic money card ID41 specifies the counter part 21 of the electronic money card 10 and the electronic money card 10 concerned, and is unique in a system. The inquiry code 42 is a code which shows the existence check inquiry to the electronic money card 10 from the counter part 21.
[0130]The issue financial institution branch code 413 electronic money card ID41 indicates the branch office of the issue financial institution 26 which published the electronic money card 10 concerned to be, It consists of the issue bank code 412 which shows the issue financial institution 26 where an issue financial institution branch belongs, the country code 411 which shows the country where the issue financial institution 26 belongs, and others 414 which are other data.
[0131]Drawing 10 is a data content of existence Acknowledgement 50 which transmits to the counter part 21 from the electronic money card 10 to the existence check inquiry to the electronic money card 10.
[0132]Electronic money card ID51 is the same ID as electronic money card ID41. The geographic coordinate 52 is geographic coordinate information the electronic money card 10 indicates the current position of the electronic money card 10 received from the GPS system (satellite positioning system by an artificial satellite) to be. The time of origin 53 is time when the electronic money card 10 transmits existence Acknowledgement 50, and the information to a time second and micro second is stored. It is shown that the answering cord 54 is response data from the electronic money card 10 to the existence check inquiry from the counter part 21.
[0133]Drawing 12 is a data content of the existence check spontaneous dispatch 60 which transmits to the counter part 21 from the electronic money card 10, and electronic money card ID61 is the same as that of electronic money card ID41. The geographic coordinate 62 is the information on the same meaning as the geographic coordinate 52. The time of origin 63 is the information on the same meaning as the time of origin 53. The spontaneous calling code 64 shows without the existence check inquiry from the counter part 21 that it is the existence check which transmitted to the target on the other hand from the electronic money card 10.
[0134]Drawing 13 is a data content of the stall 70 which transmits to the electronic money card 10, in order to connect the stop of the existence check inquiry to the electronic money card 10 from the counter part 21. Electronic money card ID71 is the same as that of electronic money card ID41. The stall time 72 shows the time interval which stops an existence check inquiry. The stall code 73 shows a stall.
[0135]Drawing 14 is a figure showing the dealings function of a class division and other opportunities of the stall of the electronic money card 10, and has from the 1st class to the 3rd class as a class of a stall, and the dealings or communication with the urgent accepting device 23 is attained also in which class. However, dealings with the store machine 20 are forbidden in the stall mode of the 1st class. The input of a password is forbidden in the stall mode of the 1st class and the 2nd class.
[0136]If the electronic money card 10 carries out the short-time depression of the power supply ON switch, it will serve as a power turn, if a depression is carried out for a long time, it will be a power turn and dealings or communication only with the urgent accepting device 23 will be attained. Even if it pushes a power supply ON switch into a power turn for a long time, dealings or communication only with the urgent accepting device 23 is attained.
[0137]Drawing 15 is a data content of the SOS dispatch directions 80 which transmit to the artificial satellite 25 from the loss theft center 24. Artificial satellite ID81 is a code which specifies the artificial satellite 25 which receives the SOS dispatch directions 80. The SOS dispatch instruction codes 82 are contents which direct broadcasting of SOS dispatch directions to the electronic money card 10 of electronic money card ID83 which is an instruction content and suited the loss theft to the artificial satellite 25. Electronic money card ID83 is electronic money card ID of the electronic money card 10 which the report was formed as having suited the loss theft and was received.
[0138]Drawing 16 is a data content of the SOS dispatch directions broadcasting 90 which broadcasts SOS dispatch directions from the artificial satellite 25 to the electronic money card 10 of electronic money card ID83 which suited the loss theft. The SOS dispatch instruction code 91 shows that this broadcasting is SOS dispatch directions. It is shown that electronic money card ID92 is the SOS dispatch directions to the electronic money card 10 with this ID.
[0139]Drawing 17 is a data content of the SOS stop instruction 100 which transmits to the artificial satellite 25 from the loss theft center 24. Artificial satellite ID101 is a code which specifies the artificial satellite 25 which receives the SOS stop instruction 100. The SOS stop instruction code 102 is an instruction content over the artificial satellite 25, and is contents which direct broadcasting of SOS stop instruction to the electronic money card 10 of electronic money card ID103.

[0140]Drawing 18 is a data content of the SOS stop instruction broadcasting 150 which broadcasts SOS stop instruction from the artificial satellite 25 to the electronic money card 10 of electronic money card ID152. The SOS stop instruction code 151 shows that this broadcasting is SOS stop instruction. It is shown that electronic money card ID152 is the SOS stop instruction to ********** 10 with this ID.
[0141]Drawing 19 is a data content of SOS160 which the electronic money card 1 of electronic money card ID92 (= electronic money card ID162) to which SOS dispatch was directed by the SOS dispatch directions broadcasting 90 from the artificial satellite 25 broadcasts. The SOS code 161 shows that this broadcasting is SOS. Electronic money card ID162 is electronic money card ID of the electronic money card 10 which has broadcast SOS. The geographic coordinate 163 is geographic coordinate information the electronic money card 10 concerned indicates the current position of the electronic money card 10 received from the GPS system to be. The time of origin 164 is time when the electronic money card 10 broadcasts SOS, and the information to a time second and micro second is stored. The storing electronic money 165 enciphers the electronic money which the electronic money card 10 concerned stores. In addition, the stored data 166 enciphers stored data other than electronic money 165 which the electronic money card 10 concerned stores.
[0142]Drawing 20 is a data content of the urgent part 22. 171 is data for options. Electronic money card ID172 is electronic money card ID, and can store two or more electronic money card ID. The urgent accepting device telephone number 173 is a telephone number of an urgent accepting device.
[0143]Drawing 11 is a data content of the functional lowest over the electronic money card 10 from the counter part 21, it comprises electronic money card ID181 and the functional resumption code 182, and the stall state up to the 3rd class is canceled of the 1st class according to the contents of the functional resumption code 182.
[0144]Drawing 21 is a flow chart which shows the basic motion in connection with loss theft prevention of the electronic money card 10.
[0145]The electronic money card 10 is provided with the sub power supply used for the purpose of this invention, and the main power supply used for the original purpose of electronic money card 10.
[0146]When a main power supply becomes one, common processing unconditionally shown in the flow chart of drawing 30 is performed (Step 2104). And if a return is carried out from the common processing shown in drawing 30, it will shift to the operation under main power supply one shown in drawing 21.
[0147]When a main power supply turn off operation is performed during main power supply one, after connecting turning OFF a main power supply to the carrier of the electronic money card 10 with a display/sound, a main power supply is turned OFF and it ends (Steps 2101-2103).
[0148]After being in a main power supply ON state, a phenomenon waiting state is canceled. And an OFF division of which phenomenon occurred is performed.
[0149]By this OFF division, the occurring phenomenon of dealings with the ** urgent accepting device 23, the dealings with a machine besides ** / operation of the self-inside of a plane, ** shock detection, ** self-money card ID reception, money card ID reception besides **, and ** timeout ** becomes clear (Steps 2105-2110).
[0150]And processing corresponding to this occurring phenomenon is performed (Steps 2111-2116).
[0151]Henceforth, it explains individually for every occurring phenomenon of this.
[0152](1) When it is dealings with the urgent accepting device 4, as shown in drawing 22, perform common processing shown in drawing 30, and it becomes an end, i.e., a phenomenon waiting state, (Step 2201).
[0153](2) the case where performed and carried out suboperation shown in drawing 30 (Step 2301), and the return has been carried out from common processing when it is the dealings with other opportunities / operation of the self-inside of a plane -- detail flowchart **** of drawing 23 -- perform dealings of the purposes like (Step 2302). Next, it is confirmed whether a business-contacts machine is the store machine 20 (Step 2303).
[0154]When a business-contacts machine is the store machine 20, all the SOS which will be held if it is confirming whether the self-electronic money card 10 holds SOS (Step 2304) and holds also transmits to the store machine 20 which is a business-contacts machine (Step 2305). Then, SOS currently held is discarded (Step 2306) and it becomes an end, i.e., a phenomenon waiting state.
[0155]When it becomes clear not to hold SOS of the other electronic money cards 1 with the check of Step 2304, it becomes an end, i.e., a phenomenon waiting state, as it is.
[0156]When it becomes clear with the check of Step 2303 that a business-contacts machine is not the store machine

20, it becomes an end, i.e., a phenomenon waiting state, as it is.
[0157](3) When there is a shock beyond shock detection, i.e., regulation, as shown in the detail flowchart of drawing 24, let the dealings function of the self-electronic money card 10 be a 3rd-class dealings stall (Step 2401).
[0158]A 3rd-class dealings stall is in the state of asking for the input of a password in the next user's operation of the self-electronic money card 10.
[0159]Next, the data 50 of the existence check spontaneous dispatch shown in drawing 12 is sent (Step 2402). Then, the timer of T1 is set (Step 2403) and it becomes an end, i.e., a phenomenon waiting state.
[0160](4) When the data in which self-money card ID exists is received, as shown in the detail flowchart of drawing 25, analyze what kind of data received data are. The received data 40 (Step 2501) of an existence check inquiry from the counter part 21 which shows ** drawing 9 received data as a result of this analysis, ** The received data 180 (Step 2503) of the functional resumption connection from the counter part 21 shown in received-data 70(Step 2502)** drawing 21 of the stall connection from the counter part 21 shown in drawing 13, ** It is divided like the received data 90 (Step 2504) of SOS dispatch directions broadcasting from the artificial satellite 25 shown in drawing 16, and the received data 150 (Step 2505) of SOS stop instruction broadcasting from the artificial satellite 25 shown in ** drawing 18.
[0161]Henceforth, it explains individually for every received data of these.
[0162]First, when the existence check inquiry from the counter part 21 shown in drawing 9 is received (Step 2501), the timer of T1 and T2 is reset (Step 2506). And it is confirmed whether the self-electronic money card 10 is [existence check spontaneous / ******] under dispatch (Step 2507). If it is [existence check spontaneous] under dispatch, the existence check spontaneous dispatch 60 shown in drawing 12 will be sent (Step 2508). Then, the timer T1 is set (Step 2509) and it becomes an end, i.e., a phenomenon waiting state.
[0163]If the self-electronic money card 10 is not sending [be / it] existence check spontaneity as a result of the check of Step 25070, the existence Acknowledgement dispatch 50 shown in drawing 10 will be sent (Step 2510). Then, the existence Acknowledgement data 50 shown in drawing 10 is sent (Step 2513). Next, the timer T2 is set (Step 2511) and it becomes an end, i.e., a phenomenon waiting state.
[0164]Next, when the stall data 70 shown in drawing 13 from the counter part 21 is received (Step 2502), let the dealings function of the self-electronic money card 10 be a 3rd-class dealings stall (Step 2512). And the stall time 72 in the stall data 70 made into stall time is set as timer T3 (Step 2514), and it becomes an end, i.e., a phenomenon waiting state.
[0165]Next, when the functional resumption data 180 shown in drawing 11 from the counter part 21 is received, (Step 2503) and timer T3 are reset (Step 2515), and a 3rd-class dealings stall is canceled (Step 2516). Then, the existence Acknowledgement data 50 shown in drawing 10 is sent (Step 2516). Next, the timer T2 is set (Step 2518) and it becomes an end, i.e., a phenomenon waiting state.
[0166]Next, when the SOS dispatch directions broadcasting data 90 from the artificial satellite 25 shown in drawing 16 is received, let the dealings function of (Step 2504) and the self-electronic money card 10 be a 1st-class dealings stall (Step 2519). Next, the balloon built in the self-electronic money card 10 is emitted (Step 2520), and the gas too built in the emitted balloon is poured in (Step 2521). And the meaning of "please send the electronic money card 10 to the arbitrary financial institutions 26" is displayed on the display of the self-electronic money card 10 (Step 2522).
[0167]Then, the electronic money stored in the self-electronic money card 10 and other data are enciphered with an encryption method different, respectively (Step 2523), and the SOS data 160 shown in drawing 19 is sent (Step 2524). Then, the timer T4 is set (Step 2525) and it becomes an end, i.e., a phenomenon waiting state.
[0168]Next, when the SOS stop instruction broadcasting data 150 from the artificial satellite 25 shown in drawing 18 is received, the electronic money stored in (Step 2505) and the self-electronic money card 10 and other data are discarded (Step 2526). And the dealings function of the self-electronic money card 10 is made into a 1st-class dealings stall (Step 2527), and dispatch of the SOS data 160 is stopped (Step 2528).
[0169]Then, the meaning of "please send the electronic money card 10 to the arbitrary financial institutions 26" is displayed on the display of the self-electronic money card 10 (Step 2529). And the balloon currently emitted is separated from the self-electronic money card 10 (Step 2530), and the existence check spontaneous outgoing data 60 shown in drawing 12 is sent (Step 2531). Then, the timer T5 is set (Step 2532) and it becomes an end, i.e., a phenomenon waiting state.

[0170]Next, when the data in which other money card ID exists is received, as shown in the detail flowchart of drawing 27, it is analyzed what kind of data the received data are. the SOS data 160 (Step 701) which shows ** drawing 19 received data as a result of this analysis, the SOS stop instruction broadcasting data 150 (Step 2702) from the artificial satellite 25 shown in ** drawing 18, and ** -- it is divided like.

[0171]Henceforth, it explains individually for every received data of these.

[0172]First, when the SOS data 160 shown in drawing 19 is received, it confirms whether to already have held (Step 2701) and the SOS data 160 of the electronic money card 10 of the same ID as electronic money card ID162 in received data (Step 2703). If it does not hold as a result of this check, the data of the SOS data 160 is stored in the self-electronic money card 10 as it is just as it is (Step 2704). Then, the stage when the data-hold of the SOS data 160 should be reported to the carrier of the self-electronic money card 10 based on electronic money card ID of the self-electronic money card 10 is calculated (Step 2705), and the information period of the calculated result is stored in the timer T6 (Step 2706). And it becomes an end, i.e., a phenomenon waiting state.

[0173]As a result of a check at Step 2703, if it has already held, it will become an end, i.e., a phenomenon waiting state, without doing anything.

[0174]When the SOS stop instruction broadcasting data 150 from the artificial satellite 25 shown in drawing 18 is received, next, the (step 2702), It confirms whether hold the SOS data 160 of the electronic money card 10 of the same ID as electronic money card ID152 in received data (Step 2707). If it holds as a result of this check, the data of the SOS data 160 concerned currently held will be discarded (Step 2708). To the display of the self-electronic money card 10, then, the display of the meaning of "since the data of other self-electronic money cards 10 is held at the self-electronic money card 10, please send by an O year O moon O day using the urgent accepting device 23", That is, in under SOS report advice, it confirms whether to be what (Step 2709) and this SOS report advice depend on the SOS data 160 of the electronic money card 10 of electronic money card ID162 in received data (Step 2710). If that is right, SOS report advice will be stopped (Step 2711) and it will become an end, i.e., a phenomenon waiting state.

[0175]It becomes an end, i.e., a phenomenon waiting state, without [the result of a check at Step 2707, otherwise,] doing anything.

[0176]After discarding the data of the SOS data 160 in Step 2708 currently held, When the report of the data of the SOS data 160 is not made by the appointed term, (Step 2712), Without notice [the] confirms whether to be without notice [of the electronic money card 10 of the same ID as electronic money card ID152 of the SOS stop instruction broadcasting data 150 which received now] (Step 2713). As a result of this check, if that is right, a 2nd-class dealings stall will be canceled (Step 2714), and it will be considered as a 3rd-class dealings stall (Step 2715). Then, "main power supply OFF directions" is performed and it branches to operation at the time of main power supply (Step 2716) OFF.

[0177]It becomes a result of a check at Step 2713, otherwise, an end, i.e., a phenomenon waiting state.

[0178]Next, when the phenomenon of timeout is detected, as it is shown in the detail flowchart of (Step 2100) and drawing 28, the phenomenon analyzes further which timeout phenomenon it is.

[0179]Timeout of the timer T1 according [the result of this analysis] to ** shock in a timeout phenomenon (Step 2801), ** Timeout of the timers T2 from the counter part 21, such as a non-inquiry (Step 2802), ** Timeout of timer T3 without functional resumption connection (Step 2803), ** Timeout of the timer T4 under SOS dispatch (Step 2804), ** It is divided like timer T6 timeout (Step 2806) of timeout (Step 2805) **SOS report advice day arrival of the timer T5 after an SOS stop, and timeout (Step 2807) of the timer T7 of **SOS report advice expiration.

[0180]Henceforth, it explains individually for every timeout phenomenon of this.

[0181]In timeout of the timer T1 by a shock, it is made into (Step 2801) and a 3rd-class dealings stall (Step 2808). And the existence check spontaneous outgoing data 60 shown in drawing 12 is sent (Step 2809). Then, the timer T1 is set (Step 2810) and it becomes an end, i.e., a phenomenon waiting state.

[0182]In timeout of the timers T2 from the counter part 21, such as a non-inquiry, it is made into (Step 2802) and a 3rd-class dealings stall (Step 2811). And the existence check spontaneous outgoing data 60 shown in drawing 12 is sent (Step 2812). Then, the timer T2 is set (Step 2813) and it becomes an end, i.e., a phenomenon waiting state.

[0183]In timeout of timer T3 without functional resumption connection, it is made into (Step 2803) and a 3rd-class dealings stall (Step 2814). And the existence check spontaneous outgoing data 60 shown in drawing 12 is sent (Step 2815). Then, the timer T2 is set (Step 2816) and it becomes an end, i.e., a phenomenon waiting state.

[0184]In timeout of the timer T4 under SOS dispatch, it is made into (Step 2804) and a 1st-class dealings stall (Step 2817). And the SOS data 160 shown in drawing 19 is sent (Step 2818). Then, the timer T4 is set (Step 2819) and it becomes an end, i.e., a phenomenon waiting state.
[0185]In timeout of the timer T5 after an SOS stop, it is made into (Step 2805) and a 1st-class dealings stall (Step 2820). And the existence check spontaneous outgoing data 60 shown in drawing 12 is sent (Step 2821). Then, the timer T2 is set (Step 2822) and it becomes an end, i.e., a phenomenon waiting state.
[0186]In timer T6 timeout of SOS report advice day arrival, (Step 2806), It carries out to the display of the self-electronic money card 10 (Step 2823)., the display of a meaning, i.e., SOS report advice, of "since the data of other self-electronic money cards 10 is held at the self-electronic money card 10, please send by an O year O moon O day using the urgent accepting device 23" Then, a report expiration date is computed based on self-electronic money card ID, it is set as the timer T7 (Step 2824), and it becomes an end, i.e., a phenomenon waiting state.
[0187]In timeout of the timer T7 of SOS report advice expiration, it is made into (Step 2807) and a 2nd-class dealings stall (Step 2825). And the display of the self-electronic money card 10 "although the data of other self-electronic money cards 10 was held at the self-electronic money card 10, since a report was not carried out within the term by an O year O moon O day, this electronic money card 10 was made into the 2nd-class dealings stall. The meaning of please send as soon as possible using the urgent accepting device 4" is indicated (Step 2826)., i.e., SOS report expiration and report advice And it becomes an end, i.e., a phenomenon waiting state.
[0188]Next, the common processing which processes by being called from each processing of the electronic money card 10 is explained using the flow chart of drawing 30 and drawing 31.
[0189]When it is called from each processing of the electronic money card 10 and performs common processing, it is analyzed whether the state of the electronic money card 10 is in what kind of state, or what kind of transaction request it is. By this common processing, as a result of this analysis, the state of a [** / 1st class] dealings stall (Step 3001), ** the state (Step 3002) of a 2nd-class dealings stall, the state (Step 3003) of a [** / 3rd class] dealings stall, the dealings demand (Step 3004) with the ** urgent accepting device 23, and ** -- in addition to this (Step 3005) -- ** -- it is divided like.
[0190]Henceforth, it explains individually for every state of this.
[0191]In the case of the state of a 1st-class dealings stall, to the display of (Step 3001) and this electronic money card 10 First, the display of the meaning of "please bring this electronic money card 10 to a nearby financial institution", That is, bringing advice to the financial institution 26 is carried out (Step 30060), and "main power supply OFF directions" is performed that a main power supply should be turned off (Step 3007).
[0192]Next, in the case of the state of a 2nd-class dealings stall, it confirms whether to be the dealings demand with (Step 3002) and the urgent accepting device 23 (Step 3008). If it is the dealings demand with the urgent accepting device 23, a session with the urgent accepting device 23 will be established (Step 3009), If all the SOS data which the electronic money card 10 concerned is holding is transmitted to the urgent accepting device 23 (Step 3010) and it finishes transmitting, a session with the urgent accepting device 23 will be released (Step 3011). Next, all the SOS data under maintenance is discarded (Step 3012), a 2nd-class dealings stall is canceled (Step 3013), and it is considered as a 3rd-class dealings stall (Step 3014). And "main power supply OFF directions" is performed that a main power supply should be turned off (Step 3015).
[0193]In the check of being the dealings demand with the urgent accepting device 23 in Step 3008, when it is not the dealings demand with the urgent accepting device 23, the data of other self-electronic money cards 10 is held at the display of the self-electronic money card 10 at the "self-electronic money card 10, but. O Since a report was not carried out within the term by a year O moon O day, this electronic money card 10 serves as a 2nd-class dealings stall. The meaning of please send as soon as possible using the urgent accepting device 23" is indicated (Step 3016)., i.e., SOS report expiration and report advice And a return is carried out to call origin.
[0194]Next, in the case of the state of a 3rd-class dealings stall, the input of (Step 3003) and a password is required (Step 3017). And it confirms whether the entered password is a regular password (Step 3018), when it is a regular password, a 3rd-class dealings stall is canceled (Step 3022), and a return is carried out to call origin.
[0195]However, when the entered password is not a regular password, the continuously mistaken number of times is counted and it is confirmed whether this count reached the regular number of times (Step 3019). When the number of times of a continuous error has reached the number of times of regulation as a result of the check, it is considered as a

1st-class dealings stall (Step 3020). And "main power supply OFF directions" is performed that a main power supply should be turned off.

[0196]When the number of times of a continuous error has not reached the number of times of regulation as a result of the check at Step 3019, it returns to Step 3018 that a password should be required again.

[0197]In the dealings demand with the urgent accepting device 23, next, the (step 3004), If a session with the urgent accepting device 23 is established (Step 3023), all the SOS data which the electronic money card 10 concerned is holding is transmitted to the urgent accepting device 23 (Step 3024) and it finishes transmitting, a session with the urgent accepting device 23 will be released (Step 3025). Next, all the SOS data under maintenance is discarded (Step 3026), and "main power supply OFF directions" is performed that a main power supply should be turned off (Step 3027).

[0198]In the case of others, it confirms whether to be (Step 3005) and "main power supply ON operation" (Step 3028), and if that is right, it branches to "Step 3017 of password demand"", and if that is not right, a return will be carried out to call origin.

[0199]The above is operation about the loss theft preventive function of the electronic money card 10.

[0200]Drawing 32 - drawing 34 are flow charts which show operation of the counter part 21. Hereafter, operation of the counter part 21 is explained below.

[0201]The power supply of the counter part 21 is one power supply, and is always an ON state fundamentally.

[0202]In operation of the counter part 21, it is standing by in the phenomenon waiting state, and when this waiting state is canceled, operation is started. And an OFF division of which phenomenon occurred is performed. Reception of as opposed to ** power turn (Step 3201) and ** inquiry by this OFF division of an existence Acknowledgement (Step 3202), ** Reception of the electronic money card's 10 existence check spontaneous outgoing data 60 (Step 3203), ** The occurring phenomenon of demand [of the stall from a user] (Step 3204), demand [of the stall release from ** user] (Step 3205), demand [of the war readiness release from ** user] (Step 3206), ** timeout (Steps 3207-3211), and ** power OFF ** becomes clear.

[0203]Henceforth, it explains individually for every occurring phenomenon of this.

[0204]First, when one [a power supply], the data of the existence check inquiry 40 shown in (Step 3201) and drawing 9 is transmitted to the electronic money card 10 (Step 3212). Then, the timer T10 is set (Step 3213) and it becomes an end, i.e., a phenomenon waiting state.

[0205]Next, in the reception of the existence Acknowledgement data 50 to the inquiry shown in drawing 10, it confirms whether to be (Step 3202) and war readiness (Step 3124). If it is war readiness, the meaning of "receiving the response to an existence check inquiry" will be displayed for the report of the response data 50 reception to an existence check inquiry on the display of the counter part 21 (Step 3215). This display is not cared about as a numeric code, when the display surface product of a display is small. When a display cannot be provided, a sound, the number of times of vibration, etc. may report. Then, the timer T11 is set (Step 3216) and it becomes an end, i.e., a phenomenon waiting state.

[0206]If it is not war readiness, the timer T9 will be set, and the timer T10 will be reset (Step 3217), and it will become an end, i.e., a phenomenon waiting state.

[0207]In reception of the electronic money card's 1 shown in drawing 12 existence check spontaneous outgoing data 60, next, the (step 3203), The timer T9 and the timer T10 are reset (Step 3218), the meaning of "spontaneous dispatch existence check reception" displays on the display of the counter part 21 (Step 3219), and the existence check inquiry data 40 shown in drawing 9 below is transmitted to the electronic money card 10 (Step 3220). And in order to decide which timer is set, it confirms whether to be war readiness (Step 3221).

[0208]If it is war readiness, the timer T11 will be set (Step 3222) and it will become an end, i.e., a phenomenon waiting state.

[0209]If it is not war readiness, the timer T10 will be set (Step 3223) and it will become an end, i.e., a phenomenon waiting state.

[0210]Next, in the demand of the stall from a user, (Step 3204) and the stall data 70 shown in drawing 13 are transmitted to the electronic money card 10 (Step 3224). And timer T3 is set by making into T3 time to the resumption which the user set up (Step 3225), the timer T9 and the timer T10 are reset (Step 3226), and it becomes an end, i.e., a phenomenon waiting state.

[0211]next, the case of a demand of the stall release from a user -- (Step 3205) -- it confirms whether to be under [stall] ****** just to make sure (Step 3227). If it is during a stall, the functional resumption data 180 shown in drawing 21 will be transmitted to the electronic money card 10 (Step 3228). Then, the timer T8 is set (Step 3229) and it becomes an end, i.e., a phenomenon waiting state.
[0212]If it is not during a stall, it will become an end, i.e., a phenomenon waiting state, without doing anything.
[0213]Next, in the demand of the war readiness release from a user, (Step 3206) and war readiness are canceled (Step 3230), and it becomes an end, i.e., a phenomenon waiting state, after that.
[0214]In timeout, there are five kinds, T3, T8, T9, T10, and T11.
[0215]** Timeout of timer T3 which tells that time to complete the time of a stall and resume a function came (Step 3207), ** The timeout of the timer T8 which tells that the response was not able to be received from the electronic money card 10 to within a time [regular] after functional resumption connection (Step 3208), ** As opposed to the timeout (Step 3209) of the timer T9 which tells that the time which asks an existence check to the electronic money card 10 came, and an inquiry of the existence check to the ** electronic money card 10, It is under [timeout / which tells that the response was not able to be received from the electronic money card 10 to within a time / regular / of the timer T10 / (Step 3210) and ** war readiness] setting, It is classified like the timeout (Step 3211) of the timer T11 which tells that the time which asks an existence check to the electronic money card 10 came.
[0216]Henceforth, it explains individually for this the timeout of every.
[0217]First, the time of a stall is completed and, in timeout of timer T3 which tells that time to resume a function came, (Step 3207) and the functional resumption data 150 shown in drawing 21 are transmitted to the electronic money card 10 (Step 3231). Then, the timer T8 is set (Step 3232) and it becomes an end, i.e., a phenomenon waiting state.
[0218]In the timeout of the timer T8 which tells that the response was not able to be received from the electronic money card 10 to within a time [regular] after functional resumption connection, next, the (step 3208), The meaning of "having no response to the functional resumption connection from the electronic money card 10" is displayed on the display of the counter part 21 (Step 3233), and it is considered as war readiness (Step 3234). Then, it becomes an end, i.e., a phenomenon waiting state.
[0219]Next, in the timeout of the timer T9 which tells that the time which asks an existence check to the electronic money card 10 came, (Step 3209) and the existence check inquiry data 40 shown in drawing 9 are transmitted to the electronic money card 10 (Step 3235). Then, the timer T10 is set (Step 3236) and it becomes an end, i.e., a phenomenon waiting state.
[0220]In the timeout of the timer T10 which tells that it was not able to receive from the electronic money card 10 to within a time [of regulation of the response], to an inquiry of the existence check to the electronic money card 10 Next, the (step 3210), The meaning of "having the electronic money card 10 to no response to an inquiry of an existence check" is displayed on the display of the counter part 21 (Step 3237), and it is considered as war readiness (Step 3238). Then, it becomes an end, i.e., a phenomenon waiting state.
[0221]In the timeout of the timer T11 which tells that the time which asks an existence check to the electronic money card 10 into war readiness came, (Step 3211) and the existence check inquiry data 40 shown in drawing 9 are transmitted to the electronic money card 10 (Step 3239). Then, the timer T11 is set (Step 3240) and it becomes an end, i.e., a phenomenon waiting state.
[0222]In the case of power OFF, it ends at the last, without doing anything.
[0223]Drawing 35 is a flow chart about operation of the urgent accepting device 23. Operation of the urgent accepting device 23 is explained below using drawing 35.
[0224]In operation of the urgent accepting device 23, it is always in the state of the waiting for reception of a call signal. And when a call signal is received, an OFF division of the call from which apparatus is performed, ** it is directly based on insertion to the urgent accepting device 23 of the call (Step 3501) from telephone, and the ** urgent part 22 -- it calls (Step 3501) and is kicked by OFF, without the call (Step 3503) from the ** electronic money card 10.
[0225]Henceforth, it explains individually for this the call of every.
[0226]First, in the case of the call from telephone, a session is established between (Step 3501) and telephone (Step 3504), and if data is received (Step 3505) and it finishes receiving from telephone, a session with telephone will be released (Step 3506). Received data have two kinds such as loss theft electronic money card ID which is loss robbery

report data, and SOS of loss theft electronic money card 10 dispatch.
[0227]After releasing the session between telephones, the loss theft center 24 is called (Step 3507), A session will be released, if a session is established between the loss theft centers 24 (Step 3508), the data received from telephone is transmitted to the loss theft center 24 (Step 3509) and it finishes transmitting (Step 3510). Then, it will be in the reception waiting state of an end, i.e., a call signal.
[0228]In the case of the call by the direct insertion to the urgent accepting device 23 of the urgent part 22, (Step 3501), 1 or all electronic money card ID that are registered are displayed on the display of the urgent accepting device 23 at the urgent part 22, and one electronic money card ID sent as the electronic money card 10 with a loss theft is determined (Step 3511). Then, operation after Step 3507 which discharged the urgent part 22 (Step 3512) and mentioned above determined electronic money card ID as send data is performed.
[0229]In the case of the call from the electronic money card 10, next, the (step 3503), A session is established between the electronic money cards 10 concerned (Step 3513), and if data is received (Step 3514) and it finishes receiving from the electronic money card 10, a session with the electronic money card 11 will be released (Step 3515). Then, operation after Step 3507 which mentioned above the data received from the electronic money card 10 as send data is performed.
[0230]Drawing 36 and drawing 37 are flow charts which show operation of the loss theft center 24. Operation of the loss theft center 24 is explained below using drawing 36 and drawing 37.
[0231]In operation of the loss theft center 24, it is always in the state of the waiting for reception of the call signal from the urgent accepting device 23. And if a session is established between (Step 3601) and the urgent accepting device 23 (Step 3602), data is received from the urgent accepting device 23 (Step 3603) and it finishes receiving when a call signal is received, a session with the urgent accepting device 23 will be released (Step 3604). Then, when it is electronic money card ID (Step 3605), the classification, i.e., ** received data, of the received data, each operation in case ** received data are SOS data (Step 3606) is performed.
[0232]Henceforth, it explains individually for this the operation of every.
[0233]First, since it is a loss robbery report when received data are electronic money card ID (Step 3605), it is confirmed whether electronic money card ID where the report is made or which had the report in the loss theft database is registered (Step 3607). When not registering with a loss theft database, it is confirmed whether electronic money card ID where this incident was solved or which had the report in the solution database is registered (Step 3608). Only when not registering with both a loss theft database and a solution database, electronic money card ID which had the report in the loss theft database is registered (Step 3609). And it progresses to Step 3610.
[0234]When it does not register with a loss theft database and registers with the solution database, since this incident is solved, it becomes an end, i.e., the call signal reception waiting state from the urgent accepting device 23.
[0235]Since it means having already received the loss robbery report of this electronic money card ID when the check in Step 3607 registers with the loss theft database, it becomes an end, i.e., the call signal reception waiting state from the urgent accepting device 23, without doing anything.
[0236]When received data are the SOS data 160 shown in drawing 19, in the case of the report of the SOS data 120, next, the (step 3606), It is confirmed whether electronic money card ID162 in the SOS data 160 which had the report whether the report is carried out and now is registered into the loss theft database (Step 3611). When registering with the loss theft database, The information on electronic money card ID162 relation in the SOS data 160 with a report is deleted from a loss theft database (Step 3612), and the information on electronic money card ID162 relation in the SOS data 160 with a report is registered into a solution database (Step 3613). And it progresses to Step 3610.
[0237]When it becomes clear that it does not register with a loss theft database with the check of Step 3611, it is confirmed whether the information on electronic money card ID162 relation in the SOS data 160 which had the report further is registered into the solution database (Step 3614). When not registering with a solution database, the information on electronic money card ID162 relation in the SOS data 160 with a report is registered into a solution database (Step 3615), and it progresses to Step 3610.
[0238]While the carrier of the electronic money card 10 which sent the SOS data 160 with a report has not noticed the loss theft of the electronic money card 10 concerned, the electronic money card 10 concerned sends the SOS data 160, and the electronic money card 10 which received this sends this case. However, there cannot be this [no]. Because, it is because there is a report of a loss theft, SOS data dispatch directions are taken out from the artificial satellite 25

and SOS data is sent only by this. However, it is the fail-safe treatment for a sense.
[0239]Since the SOS data 160 concerned is a meaning which the report is already made when it becomes clear that it registers with the solution database as a result of a check at Step 3614, it becomes an end, i.e., the call signal reception waiting state from the urgent accepting device 23, without doing anything.
[0240]Next, operation of the loss theft center 24 after Step 3610 is explained.
[0241]First, a session is established between the artificial satellites 25 (Step 3610). When it is ** loss robbery report, there are two kinds in the case of being a report of **SOS120 of subsequent operations.
[0242]Henceforth, it explains individually for this the operation of every.
[0243]First, when it is a loss robbery report, in order to make the SOS data 160 send to the electronic money card 10 of electronic money card ID with (Step 3616) and a report, The SOS dispatch indicative data 80 shown in drawing 15 is transmitted to the artificial satellite 25 (Step 3617), and the session between the artificial satellites 25 is released after that (Step 3618). Next, a session is established among the issue financial institutions 26 of the electronic money card 10 of electronic money card ID with a report (Step 3619), If the loss theft of the electronic money card 10 of electronic money card ID with a report is connected (Step 3620) and it finishes connecting, the session between the issue financial institutions 26 will be released (Step 3621), and it becomes an end, i.e., the call signal reception waiting state from the urgent accepting device 23, after that.
[0244]Next, when it is a report of SOS120, in order to make the electronic money card 10 of electronic money card ID with (Step 3622) and a report stop dispatch of the SOS data 160, The SOS stop instruction data 100 shown in drawing 17 is transmitted to the artificial satellite 25 (Step 3623), and the session between the artificial satellites 25 is released after that (Step 3624). Next, a session is established among the issue financial institutions 26 of the electronic money card 10 of electronic money card ID with a report (Step 3625), The electronic money and the other data which the electronic money card 10 of electronic money card ID with a loss theft held are transmitted to the issue financial institution 26 (Step 3626), If it finishes transmitting, the session between the issue financial institutions 26 will be released (Step 3627), and it becomes an end, i.e., the call signal reception waiting state from the urgent accepting device 23, after that.
[0245]Drawing 38 is a flow chart which shows operation of the artificial satellite 25.
[0246]In operation of the artificial satellite 25, it is standing by in the phenomenon waiting state, and when this waiting state is canceled, operation is started. And an OFF division of which phenomenon occurred is performed. By this OFF division, the occurring phenomenon of timeout (Step 3802-3803) of the call (Step 3801) from ** loss theft center 24 and ** timer becomes clear.
[0247]Henceforth, it explains individually for every occurring phenomenon of this.
[0248]In the case of the call from the loss theft center 24, first, the (step 3801), A session is established between the loss theft centers 24 (Step 3804), and if data is received (Step 3805) and it finishes receiving from the loss theft center 24, a session with the loss theft center 24 will be released (Step 3806). Then, the data received from the loss theft center 24 confirms whether to be the SOS dispatch indicative data 80 shown in drawing 15 (Step 3807). If it is the SOS dispatch indicative data 80, the SOS dispatch directions broadcasting data 90 shown in drawing 16 will be broadcast (Step 3808). Then, the timer T12 is set (Step 3809) and it will be in the state waiting for a call from the end 24, i.e., a loss theft center.
[0249]When the received data is not the SOS dispatch indicative data 80 as a result of a check at Step 3807 (i.e., when it is the SOS stop instruction data 100 shown in drawing 17), the SOS stop instruction broadcasting 110 shown in drawing 11 is broadcast (Step 3810). Then, the timer T13 is set (Step 3811) and it will be in the state waiting for a call from the end 24, i.e., a loss theft center.
[0250]Next, timeout is classified, without the timeout for broadcasting **SOS dispatch directions broadcasting data 90, and the timeout for broadcasting **SOS stop instruction broadcasting 150.
[0251]Henceforth, it explains individually for this the timeout of every.
[0252]First, in timeout of the timer T12 for broadcasting the SOS dispatch directions broadcasting data 90, the (Step 3802) SOS dispatch directions broadcasting data 90 is broadcast (Step 3812). Then, the timer T12 is set (Step 3813) and it will be in the state waiting for a call from the end 24, i.e., a loss theft center.
[0253]Next, in timeout of the timer T13 for broadcasting the SOS stop instruction broadcasting data 150, the (Step 3803) SOS stop instruction broadcasting data 150 is broadcast (Step 3814). Then, the timer T13 is set (Step 3815) and

it will be in the state waiting for a call from the end 24, i.e., a loss theft center.
[0254]Idle time, such as a base station of a PHS telephone network or a vertical-retrace-line period of a television signal, is used, and it may be made to perform SOS dispatch directions etc. instead of using the artificial satellite 25.
[0255]
[Effect of the Invention]According to this invention, the electronized currency stored by the electronic money dealings machine or electronic money dealings machine which suited loss and a theft, and other data are easily recoverable so that clearly from the above explanation.
[0256]Loss by mislaying after the fall from the body of an electronic money dealings machine or use can be prevented.
[0257]it goes through a prescribed period -- the input of the password which is alike, suspends the function of an electronic money dealings machine, and is changed for between [every] homonomy scheduled time -- the stall of an electronic money dealings machine -- it may cancel -- it can accumulate and the safety of an electronic money dealings machine can be improved now.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a system configuration figure showing an embodiment of the invention.
[Drawing 2]It is a figure showing the operation-sides side composition of an electronic money dealings machine.
[Drawing 3]It is a block diagram showing the internal configuration of an electronic money dealings machine.
[Drawing 4]It is a figure showing the outline of processing in the case of trading between an electronic money dealings machine and POS.
[Drawing 5]It is a system configuration figure showing the composition of the principal part of a loss theft preventive function.
[Drawing 6]It is a functional block which shows the composition of a counter part.
[Drawing 7]It is a figure showing Example 1 of an effective password for 24 hours.
[Drawing 8]It is a figure showing Example 2 of an effective password for 24 hours.
[Drawing 9]It is a lineblock diagram of existence check inquiry data (counter part -> electronic money card).
[Drawing 10]It is a lineblock diagram of the existence Acknowledgement data (electronic money card -> counter part) based on an inquiry.
[Drawing 11]It is a lineblock diagram of functional resumption data (counter part -> electronic money card).
[Drawing 12]It is a lineblock diagram of the existence check spontaneous outgoing data (electronic money card -> counter part) based on an inquiry.
[Drawing 13]It is a lineblock diagram of stall data (counter part -> electronic money card).
[Drawing 14]It is an explanatory view showing the contents of the dealings stall.
[Drawing 15]It is a lineblock diagram of SOS dispatch indicative data (loss theft center -> artificial satellite).
[Drawing 16]It is a lineblock diagram of SOS dispatch directions broadcasting data (artificial satellite -> electronic money card).
[Drawing 17]It is a lineblock diagram of SOS stop instruction data (loss theft center -> artificial satellite).
[Drawing 18]It is a lineblock diagram of SOS stop instruction and SOS abandonment indicative data (artificial satellite -> electronic money card).
[Drawing 19]It is a lineblock diagram of SOS data (electronic money card -> electronic money card).
[Drawing 20]It is a lineblock diagram showing the data content of an urgent part.
[Drawing 21]It is a flow chart which shows the basic motion in connection with loss theft prevention of an electronic money card.
[Drawing 22]It is a flow chart which shows processing of transactions with an urgent accepting device.
[Drawing 23]It is a flow chart which shows another opportunity / self-inside-of-a-plane processing of transactions.
[Drawing 24]It is a flow chart which shows the processing corresponding to shock detection.
[Drawing 25]It is a flow chart which shows the processing at the time of self-card ID reception.
[Drawing 26]It is a flow chart which shows a continuation of drawing 25.

[Drawing 27]It is a flow chart which shows the processing at the time of other card ID reception.
[Drawing 28]It is a flow chart which shows time out treatment.
[Drawing 29]It is a flow chart which shows a continuation of drawing 28.
[Drawing 30]It is a flow chart which shows common processing.
[Drawing 31]It is a flow chart which shows a continuation of drawing 30.
[Drawing 32]It is a flow chart which shows operation of a counter part.
[Drawing 33]It is a flow chart which shows a continuation of drawing 32.
[Drawing 34]It is a flow chart which shows a continuation of drawing 33.
[Drawing 35]It is a flow chart which shows operation of an urgent accepting device.
[Drawing 36]It is a flow chart which shows operation of a loss theft center.
[Drawing 37]It is a flow chart which shows a continuation of drawing 36.
[Drawing 38]It is a flow chart which shows operation of an artificial satellite.
[Description of Notations]
10, 11a-11c, 12 [-- A transmitter-receiver, 146 / -- GPS 21 / -- A counter part, 22 / -- An urgent part, 23 / -- An urgent accepting device, 24 / -- A loss theft center, 25 / -- Artificial satellite.] -- An electronic money dealings machine, 13, 14 -- A POS terminal, 15 -- A network, 143,144,145

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－105627

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３３０
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｌ
Ｇ０７Ｄ　9/00	４３６	Ｇ０７Ｄ　9/00	４３６Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｃ
Ｈ０４Ｑ　7/38		Ｇ０６Ｆ　15/30	３５０

審査請求　未請求　請求項の数５　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願平8－260009

(22)出願日　平成８年(1996)９月30日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　鮫島　吉喜
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　川崎　淳
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　電子通貨取引機の紛失盗難防止方法および電子通貨取引機

(57)【要約】

【課題】　電子通貨取引機の身体からの落下や使用後の置忘れによる紛失の防止を支援すること。紛失や盗難にあった電子通貨取引機あるいは電子通貨取引機に収納されている電子化通貨やその他のデータの回収を支援すること。

【解決手段】対となる電子通貨取引機との間で微弱電波によって存在確認信号を送受し合い、電子通貨取引機からの存在確認信号が受信されなくなった状態で、当該電子通貨取引機の所有者に警告を発する機器を電子通貨取引機所有者に携帯させ、電子通貨取引の紛失、盗難を防止する。また、紛失盗難救援機関から第１の搬送周波数の無線回線を通じて自身が保有する電子化通貨の他の電子通貨取引機への移転指示を受信した時に、保有する電子化通貨を含むデータを移転データとして暗号化し、前記移転の指示とは異なる第２の搬送周波数の無線回線上に送信する手段を備える。

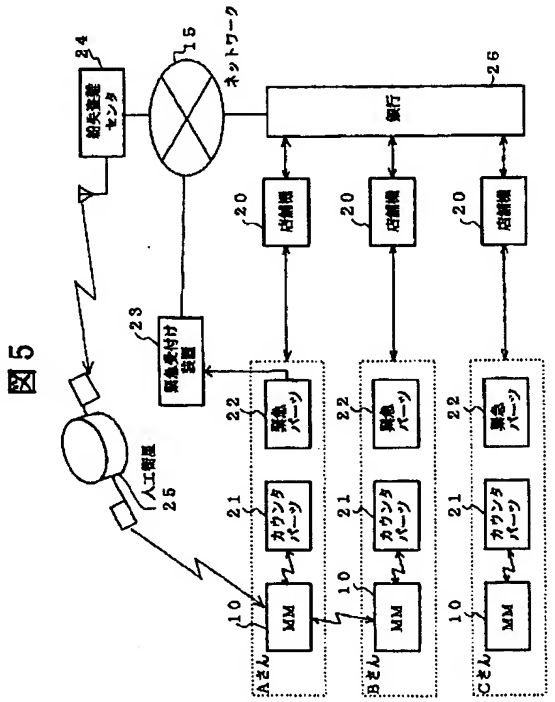


図５

【特許請求の範囲】

【請求項１】　金融機関の出納機から発行され、電子化通貨を格納した１対の電子通貨取引機同士で電子化通貨を取引する電子通貨取引の紛失盗難防止方法であって、対となる電子通貨取引機との間で微弱電波によって存在確認信号を送受し合い、電子通貨取引機からの存在確認信号が受信されなくなった状態で、当該電子通貨取引機の所有者に警告を発する機器を電子通貨取引機所有者に携帯させ、電子通貨取引の紛失、盗難を防止することを特徴とする電子通貨取引機の紛失盗難防止方法。

【請求項２】　金融機関の出納機から発行され、電子化通貨を格納した１対の電子通貨取引機同士で電子化通貨を取引する電子通貨取引機であって、

紛失盗難救援機関から第１の搬送周波数の無線回線を通じて自身が保有する電子化通貨の他の電子通貨取引機への移転指示を受信した時に、保有する電子化通貨を含むデータを移転データとして暗号化し、前記移転の指示とは異なる第２の搬送周波数の無線回線上に送信する第１の手段と、

前記第２の搬送周波数の無線回線を通じて他の電子通貨取引機から暗号化された移転データを受信した時、この他の電子通貨取引機からの移転データを保持する移転データ保持手段と、

この移転データ保持手段に保持された移転データをネットワーク経由で所定の金融機関に送信し、移転する移転処理手段と、

前記紛失盗難救援機関から前記第１の搬送周波数の無線回線を通じて移転指示停止指令を受信した時、移転データの送信を停止すると共に、自身が保有する電子化通貨を廃棄する廃棄処理手段と、を備えることを特徴とする電子通貨取引機。

【請求項３】　前記移転データを第２の搬送周波数の無線回線上に送信するに際し、自身を取引不能状態とした後に送信することを特徴とする請求項２記載の電子通貨取引機。

【請求項４】　所定時間間隔で自身を取引不能状態とし、パスワードの入力によって取引不能状態を解除する手段をさらに有することを特徴とする請求項２または３記載の電子通貨取引機。

【請求項５】　所定時間間隔で自身を取引不能状態としたときにパスワードを変更する手段をさらに有することを特徴とする請求項２または３記載の電子通貨取引機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、金融機関の出納機から発行され、電子化通貨を格納した１対の電子通貨取引機同士で電子化通貨を取引する電子通貨取引システムの電子通貨取引機の紛失盗難防止方法および電子通貨取引機に関するものであり、特に、紛失や盗難にあった電子通貨取引機を容易に発見し、あるいは紛失や盗難にあった電子通貨取引機に収納されている電子化通貨やその他のデータを容易に回収することができる電子通貨取引機の紛失盗難防止方法および電子通貨取引機に関するものである。

【０００２】

【従来の技術】従来、例えば特公平８－２７８１５号公報(発明の名称；電子資産データ移転方法)や特公平７－１１１７２３号公報(発明の名称；電子通貨システム)に開示されているように、通貨に相当する電子化通貨(電子マネー)を格納したデータ担体(電子通貨取引機)あるいは取引モジュールによって個人間あるいは個人と店舗等の非個人との間で商取引あるいは金銭貸借等の取引を可能にした技術がある。

【０００３】

【発明が解決しようとする課題】しかしながら、上記公報に開示された技術にあっては、電子通貨取引機の紛失や盗難に対しての電子通貨取引機またはその収納データの回収に考慮が払われていないという問題があった。

【０００４】本発明は上記問題を解決するためになされたものであり、その第１の目的は、電子通貨取引機の身体からの落下や使用後の置忘れによる紛失を防止することができる電子通貨取引機の紛失盗難防止方法を提供することにある。

【０００５】また、第２の目的は、紛失や盗難にあった電子通貨取引機あるいは電子通貨取引機に収納されている電子化通貨やその他のデータを容易に回収することができる電子通貨取引機を提供することにある。

【０００６】さらに、本発明の第３の目的は、電子通貨取引機の安全性を高めることができるように規定時間を経過するごとに電子通貨取引機の機能を一旦停止し、同規定時間ごとに変更されるパスワードの入力によって電子通貨取引機の機能停止を解除することができる電子通貨取引機を提供することにある。

【０００７】

【課題を解決するための手段】上記第１の目的を達成するために、本発明の電子通貨取引機の紛失盗難防止方法は、対となる電子通貨取引機との間で微弱電波によって存在確認信号を送受し合い、電子通貨取引機からの存在確認信号が受信されなくなった状態で、当該電子通貨取引機の所有者に警告を発する機器を電子通貨取引機所有者に携帯させ、電子通貨取引の紛失、盗難を防止することを特徴とする。

【０００８】また、第２の目的を達成するために、本発明の電子通貨取引機は、紛失盗難救援機関から第１の搬送周波数の無線回線を通じて自身が保有する電子化通貨の他の電子通貨取引機への移転指示を受信した時に、保有する電子化通貨を含むデータを移転データとして暗号化し、前記移転の指示とは異なる第２の搬送周波数の無線回線上に送信する第１の手段と、前記第２の搬送周波数の無線回線を通じて他の電子通貨取引機から暗号化さ

れた移転データを受信した時、この他の電子通貨取引機からの移転データを保持する移転データ保持手段と、この移転データ保持手段に保持された移転データをネットワーク経由で所定の金融機関に送信し、移転する移転処理手段と、前記紛失盗難救援機関から前記第１の搬送周波数の無線回線を通じて移転指示停止指令を受信した時、移転データの送信を停止すると共に、自身が保有する電子化通貨を廃棄する廃棄処理手段と、を備えることを特徴とする。

【０００９】ここで、移転データを第２の搬送周波数の無線回線上に送信するに際し、自身を取引不能状態とした後に送信するようにする。

【００１０】また、だい３の目的を達成するために、本発明の電子通貨取引機は、所定時間間隔で自身を取引不能状態とし、パスワードの入力によって取引不能状態を解除するようにし、さらには所定時間間隔で自身を取引不能状態としたときにパスワードを変更するようにしたことを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して詳細に説明する。

【００１２】なお、本発明の実施の形態における機器間で送受信されるデータは、特に断らない限り送受信対象機器間だけで解読できるように暗号化されている。この暗号化には公知の暗号化技術を用いる。

【００１３】図１は、本発明を適用した電子通貨取引システムの実施の形態を示すシステム構成図であり、銀行Ａの出納機から発行された電子通貨取引機（＝ＭＭ、以下、電子マネーカードという）１０および１１ａ～１１ｃと、銀行Ｂの出納機から発行された電子マネーカード１２が存在する。図１中の破線は、発行銀行との関係を明示するものである。

【００１４】このうち、電子マネーカード１０および１２は、親子関係をもたない単独の電子マネーカードであるが、電子マネーカード１１ａ～１１ｃは銀行Ａの出納機において親、子、孫の親子関係が設定されている。

【００１５】いずれの電子マネーカード１０，１１ａ～１１ｃ，１２も携帯可能に構成され、銀行の出納機あるいは他の電子マネーカード、あるいは親子関係の電子マネーカード同士、または電子化通貨ＥＭの取引が可能なＰＯＳ端末１３，１４との間で電子化通貨ＥＭの取引が可能になっている。また、銀行Ａ，Ｂはネットワーク１５で接続され、このネットワーク１５を通じて銀行間の電子化通貨ＥＭの取引が可能なように構成されている。

【００１６】但し、自分の上位機として親を持つ電子マネーカード１１ｂ，１１ｃについては、親から設定された属性によって取引が制限される。下位機は上位機から設定された属性を勝手に削除することができない。但し、属性の追加および自分で追加した属性は自由に削除することができる。

【００１７】取引される電子化通貨ＥＭは、公知の対称キー暗号表記技術を用いた暗号化アルゴリズムに従って暗号化されて取引相手に移転される。

【００１８】これら携帯可能な電子マネーカード１０，１１ａ～１１ｃ，１２は、銀行の出納機から発行されるに際して、個人の所有であることを識別情報（ＩＤ）が設定されている。

【００１９】ＰＯＳ端末１３，１４も銀行Ａ，Ｂの出納機から発行されるものであり、その発行に際しては、非個人の所有であることを識別情報（ＩＤ）が設定されている。

【００２０】電子化通貨ＥＭの取引に際しては、実線Ｓで示すように、相手機との間にセッション（通信路）が確立される。このセッション（通信路）は、ケーブル等による直接接続、光、微弱電波、電磁結合等の公知技術を利用した手段によって確立される。

【００２１】電子マネーカード１０，１１ａ～１１ｃ，１２は、予算計画に基づいた取引を支援するために、予算費目別の通貨ホルダを備えているが、この通貨ホルダの構造については外部のパーソナルコンピュータ１６，１７，１８で任意に設定できるように、パーソナルコンピュータとの通信プログラムを内蔵している。なお、当初は標準的なホルダ構造が用意されており、このうちのいずれかを選択し、必要に応じて訂正して使用する。

【００２２】電子マネーカード１０，１１ａ～１１ｃ，１２は、図２に電子マネーカード１１ａを代表して示すように、パーソナルコンピュータ１７との接続インタフェース１１０，他の電子マネーカード１２との接続インタフェース１１１およびＰＯＳ端末１９との接続インタフェース１１２を備え、さらに通貨ホルダ内の電子化通貨ＥＭの残高や取引金額等を表示する表示部１１４、支払いキー１１６、残高紹介キー１１７、受入れキー１１８、取消しキー１１９、署名キー１２０等の操作ボタンから成る機能キー部１１５、数字および英字等のキーとカーソル移動キー１２１から成る文字キー部１２２とを操作面側に備えている。

【００２３】支払いキー１１６は、相手との取引内容が合意し、実際に電子化通貨ＥＭを相手機に移転させる時に操作するキーである。なお、ＰＯＳ端末１９との間で取引する場合、この支払いキー１１６を操作する代わりに、ＰＯＳ端末１９に設置された「支払い承認キー」を操作するように構成することができる。

【００２４】残高紹介キー１１７は、通貨ホルダ内の電子化通貨ＥＭの残高を表示させるためのものであり、この残高紹介キー１１７を操作する度に次の通貨ホルダの残高が表示される。

【００２５】受入れキー１１８は、相手機から電子化通貨ＥＭを受け入れる時に操作するキーである。

【００２６】取消しキー１１９は、取引を取り消す際に操作するキーであり、この取消しキー１１９を操作する

と、相手機との間に確立していたセッションが切断される。

【００２７】署名キー１２０は、電子化通貨ＥＭの移転元の署名を相手機に送信する時に操作するキーであり、小切手等の取引時に使用する。

【００２８】図２においては、パーソナルコンピュータ１７および他の電子マネーカード１２との接続インタフェース１１０，１１１はケーブルによる接続している例を示し、ＰＯＳ端末１９との接続インタフェース１１は微弱電波によって接続している例を示しているが、これに限定されるものではない。

【００２９】但し、ＰＯＳ端末１９との接続インタフェース１１２は微弱電波によって接続した方が、不特定多数の顧客との間で電子化通貨ＥＭを取引するに際して効率的に処理を進行させる上で有効である。

【００３０】図３は、電子マネーカード１０，１１ａ～１１ｃ，１２の内部機能を示す機能ブロック図であり、大別すると、メモリ１３０、ＣＰＵ１３５，クロック／タイマ１３６、入出力インタフェース１３７、操作面の各操作キーとのキーボードインタフェース１３８、表示部インタフェース１３９、外部のパーソナルコンピュータとのインタフェース１４０、他の電子マネーカードとのインタフェース１４１、ＰＯＳ端末とのインタフェース１４２、人工衛星との通信を行うための送受信機１４４、他の電子マネーカードとの送受信を行うための送受信機１４３、後述するカウンタパーツとの送受信を行うための送受信機１４５、ＧＰＳ（人工衛星を用いた位置認識システム）による位置認識を行うためのＧＰＳ受信機１４６を備えている。

【００３１】そして、メモリ１３０内には、電子化通貨ＥＭ（電子マネー）を格納する金庫１３０１、クーポン券等の代用マネーを格納する代用マネー格納庫１３０２、取引履歴を格納する取引ログ格納庫１３０３、使途目的別の電子化通貨ＥＭの金額を格納するマネーホルダ１３０４、発行銀行ＩＤを格納する記憶領域１３０５、自機ＩＤを格納する記憶領域１３０６、上位機ＩＤを格納する記憶領域１３０７、下位機ＩＤを格納する記憶領域１３０８、電子化通貨ＥＭの使途を制限するために用いる自機の属性を格納する記憶領域１３０９、パーソナルコンピュータ通信プロの格納領域１３１０、取引機用プログラムの格納領域１３１１、これら格納領域１３１０と１３１１との間での転送データを送受するための転写領域１３１３、暗号／復号プログラムの格納領域１３１２、後述するカウンタパーツとの送受信プログラム１３１５、人工衛星との通信プログラム１３１６、他の電子マネーカードとの間での送受信プログラム１３１７、これらのプログラム１３１５，１３１６，１３１７で送受信するデータを保持する送受信データ保持領域１３１８が設けられている。

【００３２】図４は、電子マネーカード１１ｂとＰＯＳ１３との間で購入商品に対する支払いを電子化通貨ＥＭで行う場合の取引機内の処理および電子化通貨ＥＭの流れを概略的に示す説明図である。なお、図４において、個人取引機と電子マネーカードは同じである。

【００３３】電子マネーカード１１ｂの携帯者がＰＯＳ１３の設置された店舗で商品を購入し、電子マネーカード１１ｂ内の電子化通貨ＥＭで支払って取引を完了させようとする場合、電子マネーカード１１ｂの携帯者は、電子マネーカード１１ｂをＰＯＳ１３の読み取り機に接近させ、微弱電波によって電子マネーカード１１ｂとＰＯＳ１３とのセッションを確立する。

【００３４】この状態で、ＰＯＳ１３のバーコードリーダで読み取られた購入商品についての請求金額および商品名称、商品区分等の商品属性がＰＯＳ１３から送られて来たならば、電子マネーカード１１ｂは、商品区分に対応する使用項目別（使途目的別）のマネーホルダが存在するか否かを調べ、存在しない場合、あるいは存在したとしても保持金額が請求金額に満たない場合は、取引不能と判定し、電子化通貨ＥＭの支払いを不許可とする（ステップ１７０１）。

【００３５】しかし、商品区分に対応する使用項目別（使途目的別）のマネーホルダが存在し、かつその保持金額が請求金額を上回る場合は、次に、使用制限チェックを行う（ステップ１７０２）。

【００３６】詳しくは、自機属性の記憶領域１３０９に設定されている銀行の出納機からの出金の禁止／解除、１日当りの電子マネー移転限度回数、１回取引当りの限度額、１日当りの取引限度額、上位機への報告時期（月末など）、下位機携帯者の生年月日、報告上位機のＩＤなどの属性情報を取り出し、この属性情報と商品区分や商品名称、請求金額等を照合し、取引禁止条件に該当する場合は、電子化通貨ＥＭの支払いを不許可とする（ステップ１７０２）。

【００３７】取引禁止条件に該当する場合とは、例えば未成年者がタバコを購入しようとした場合を指し、その旨のメッセージと該当商品名称が表示部１１４に表示される。

【００３８】しかし、取引禁止条件に該当しない場合は、支払いボタン１１６が操作されて、購入者の購入意志が決定された条件で電子化通貨ＥＭの支払いを許可し、請求金額相当の電子化通貨ＥＭを金庫１３０１から引き出し、これを暗号化し、ＰＯＳ１３に送信する。

【００３９】電子化通貨ＥＭを受信したＰＯＳ１３は、電子化通貨ＥＭの支払いを受けた時に、領収書の発行要求があった場合は、領収書とそのＩＤを電子マネーカード１１ｂに送信する。また、クーポン券を使用する旨のメッセージを電子化通貨ＥＭの支払いを受けた時に受信していた場合は、クーポン券相当の金額を請求金額から差引き、残りを請求金額とする。そして、今回の新たな商品購入によってクーポン券を発行し、電子マネーカー

ド１１ｂに送信し、セッションを切断する。

【００４０】セッション切断後、電子マネーカード１１ｂは領収書を含む取引履歴を取引ログの記憶領域１３０３に格納して取引処理を終了する。

【００４１】なお、クーポン券を使用するか否か、および領収書を要求するか否かは商品を購入する前に予め設定しておく。これは、文字キー部１２２のキー操作によって設定する。

【００４２】図５は、本発明を適用した電子通貨取引システムにおいて紛失盗難防止機能の主要部の構成を示すシステム構成図であり、図１と同一部分は同一記号で表している。なお、以下の構成において、機器間で送受信されるデータは、特に断らない限り送受信対象機器間だけで解読できるように暗号化されている。この暗号化には公知の暗号化技術を用いる。

【００４３】図５において、１０は電子マネー等が格納されている電子マネーカードである。２１は電子マネーカード１０と一対を成し、電子マネーカード１０の紛失盗難を防止するカウンタパーツである。２２は電子マネーカード１０の緊急パーツであり、電子マネーカード１０が紛失盗難した場合の届先の電話番号が記憶されている。

【００４４】２３は電子マネーカード１の紛失盗難届けや電子マネー回収届けをする緊急受付装置、２４はは紛失盗難届けや電子マネー回収届けを受付ける紛失盗難センタ、２５は紛失盗難センタ２４からの各種指示を指示対象とされた電子マネーカード１０に対して行う人工衛星、２６は電子マネーカード１０を発行した各金融機関、２０は金融機関や公共施設等に設置されている店舗機である。

【００４５】以下に、各装置の機能概略について個別に説明する。

【００４６】（１）電子マネーカード１０

電子マネーカード１０は、前述した電子マネ取引機能の他に、紛失盗難防止のために、次の機能を備えている。

【００４７】＜紛失盗難防止のための存在確認電波の発信＞

①自身と対を成すカウンタパーツ２１からの存在確認問合せに対して、存在確認電波を発信する。

【００４８】②カウンタパーツ２１からの存在確認問合せが規定時間内に届かなかったら、自発的に存在確認電波を発信する。

【００４９】③ある程度以上の衝撃を受けたら、自発的に存在確認電波を発信する。

【００５０】また、前記②と③の場合には電子マネーカード１０は、他の電子マネーカード１０との取引きができないように一時的に取引機能を停止する。

【００５１】＜紛失盗難時におけるＳＯＳの発信と停止＞電子マネーカード１０は、人工衛星２５からのＳＯＳの発信指示または停止指示を受けてＳＯＳを発信したり停止することができる。

【００５２】紛失盗難のあった電子マネーカード１０から電子マネーを回収するために、他の電子マネーカード１０ではこの電子マネー（ＥＭ）を使用できないように、ＳＯＳのデータ中にはＳＯＳを発信した電子マネーカード１０が保有している電子マネーが暗号化されて存在する。

【００５３】また、ＳＯＳを発信した場合は他の電子マネーカード１との取引きができないように取引機能を停止する。

【００５４】さらに、ＳＯＳを停止する場合は保有している電子マネーを廃棄する。

【００５５】＜ＳＯＳの受信＞電子マネーカード１０は、他の電子マネーカード１０が発信したＳＯＳを受信することができる。

【００５６】ＳＯＳを受信した電子マネーカード１０は、自電子マネーカード１０にＳＯＳを取込み、適当な時期に自電子マネーカード１の保有者に「ＳＯＳを保持しているので届けが必要です」と振動／音／点滅等により知らせる。ＳＯＳを受信した電子マネーカード１０の保有者がある期間内にこれを届けないと、ＳＯＳを受信した電子マネーカード１０は自身の機能を停止することもある。停止させるか、停止させないかは、その所有者の銀行信用度により、金融機関が設定することができる。

【００５７】電子マネーカード１０には、暗号化された本人の写真が格納されており、すり替え不能である。

【００５８】＜電波の強さ＞電子マネーカード１０がカウンタパーツ２１に送信する電波の出力は、カウンタパーツ２２が発信する存在確認問合せ電波よりも大きい。

【００５９】（２）カウンタパーツ２１

＜カウンタパーツ２１の目的＞カウンタパーツ２１は、電子マネーカード１０の紛失早期検知用のものであり、電子マネーカード１０と一対を成す。電子マネーカード１０が保有者の身体から規定距離または規定時間離れたことを検知して保有者に知らせる。

【００６０】通常はアクセサリ／腕時計／メガネ／ベルトバックル等の常に保有者の身体と携帯するものに装着される。

【００６１】図６は、カウンタパーツ２１の構成を示す機能ブロック図であり、ＣＰＵ２１０、メモリ内に格納された他の電子マネーカードとの取引機間送受信プログラム２１１、液晶表示器（ＬＣＤ）２１２、ブザー２１４とのインタフェース２１３、対を成す電子マネーカード１０との送受信機２１６、この送受信機２１６とのインタフェース、アンテナ２１７、服装や携帯品の一部に固定するための金具２１８、捜索ボタン２１９を備えている。

【００６２】＜近傍存在確認機能＞カウンタパーツ２１は、規定時間間隔で対応する電子マネーカード１０に対

して電波によりその存在確認問合せを行う。問合せを受けた電子マネーカード１０は、上述の自カードの存在確認を応答する。電子マネーカード１０からの応答を規定時間内に受信できなかった場合は、カウンタパーツ２１自身を振動／音／点滅等させてカウンタパーツ２１の保有者にその旨を知らせる。

【００６３】また、電子マネーカード１０が自発的に発信した存在確認を受信した場合も、カウンタパーツ２１自身を振動／音／点滅等させ、カウンタパーツ２１の保有者にその旨を知らせる。

【００６４】＜近傍存在確認機能の一時停止＞保有者は、一時的に近傍存在確認機能を停止させることができる。この場合、カウンタパーツ２１は、自分自身と対を成す電子マネーカード１０に対してその旨連絡する。

【００６５】＜形態＞電子マネーカード１０の保有者は、通常、電子マネーカード１０とともにカウンタパーツ２１を携帯している。カウンタパーツ２１は、通常は身体から離れにくいように身体に携帯されている。また、カウンタパーツ２１がネックレス、指輪、腕輪、鼻輪、メガネ、ベルトバックル等のアクセサリ類に予め組込んだ形態の携帯も考えられる。

【００６６】この場合、電子マネーカード１０から受信した存在確認により受信した方位／距離データを表示するように機能アップすることができる。また、電子マネーカード１０に近づく程、振動／音／点滅等を受信電波の強度によって制御する個ともできる。

【００６７】なお、カウンタパーツ２１自身の紛失も考えられるため、１つの電子マネーカード１０ごとに２ケ以上を身辺に携帯することが望ましい。

【００６８】（３）緊急パーツ２２
＜目的／機能＞緊急パーツ２２は、電子マネーカード１０の紛失盗難に対しての届け用テレフォンカードである。

【００６９】１つまたは複数の電子マネーカードＩＤ及び届先である紛失盗難センタ２４の電話番号が設定されている。緊急パーツ２２を緊急受付装置２３または電話機に差込むことによって紛失盗難センタ２４に電子マネーカード１０の紛失盗難を届けることができる。

【００７０】緊急パーツ２２は、廉価なものであるので、１つの電子マネーカード１０または家族が保有する全電子マネーカード１０に対して同一内容の緊急パーツ２２を１０枚程度を保有し、各所に点在させておくことが望ましい。

【００７１】この点在により、空き巣／強盗／脅迫等によって、電子マネーカード１０とカウンタパーツ２１がこの緊急パーツ２２と一緒に奪われても、どこかには奪われなかった緊急パーツ２２を残しておくことができる。

【００７２】また、電子マネーカード１０の紛失盗難にあったときに即座に届けられるようにするため、緊急パーツ２２を持ち歩くことが望ましい。

【００７３】（４）緊急受付装置２３
＜目的＞緊急受付装置２３は、紛失盗難にあった電子マネーカード１０を紛失盗難センタ２４に届けるための装置である。また、紛失盗難にあった電子マネーカード１０から受信したＳＯＳを紛失盗難センタ２４に届けるための装置でもある。

【００７４】＜機能＞緊急パーツ２２を緊急受付装置２３に挿入すると、緊急受付装置２３は挿入された緊急パーツ２２に登録されている１または複数の電子マネーカードＩＤを緊急受付装置２３の表示部に表示する。そして緊急パーツ２２を挿入した人によって選択された電子マネーカードＩＤが紛失盗難となった電子マネーカード１０の電子マネーカードＩＤとして紛失盗難センタ２４に届けられる。

【００７５】＜設置場所＞緊急受付装置２３は、金融機関の本支店，郵便局，警察署交番，駅，病院，公共施設等に設置される。

【００７６】（５）紛失盗難センタ２４
＜目的＞紛失盗難センタ２４は、紛失盗難にあった電子マネーカード１０の管理センタである。

【００７７】＜機能＞紛失盗難センタ２４は、緊急受付装置２３から届け出のあった電子マネーカードＩＤの電子マネーカード１０に対し、ＳＯＳを発信させるよう人工衛星２５に指示し、また当該電子マネーカード１０を発行した金融機関２６にその旨を連絡する。

【００７８】また、紛失盗難にあった電子マネーカード１０の保有していた電子マネーを回収した場合、その電子マネーカード１０にＳＯＳの発信を停止させるよう人工衛星２５に指示し、また当該電子マネーカード１０を発行した金融機関２６にその旨を連絡する。

【００７９】（６）人工衛星２５
＜目的＞人工衛星２５は、紛失盗難センタ２４からの指示を電子マネーカード１０に伝達する中継装置である。

【００８０】＜機能＞人工衛星２５は、緊急受付装置２３から指示された電子マネーカードＩＤの電子マネーカード１０に対してＳＯＳの発信または停止の指示をする。

【００８１】以下に、紛失盗難防止機能の概要を説明する。

【００８２】まず、紛失盗難防止について説明する。

【００８３】（１）ケース１＜通常＞
カウンタパーツ２２は、電子マネーカード１０に対して図９に示す存在確認の問合せを規定の時間間隔で常時行っている。この問合せに対して、電子マネーカード１０はカウンタパーツ２１に対して図１０に示す存在確認応答を行う。したがって、それぞれが発信する電波が届く範囲においては相互に相手が自機の近傍に存在していることを確認できる。

【００８４】（２）ケース２＜電子マネーカード１０の

落下により、その衝撃の大きさが規定以上である場合＞電子マネーカード１０の保有者が歩行中に電子マネーカード１０を落し、電子マネーカード１０が受けた落下衝撃が規定以上である場合、電子マネーカード１０自身は図１２に示す存在確認自発発信のデータを自発的に発信する。

【００８５】カウンタパーツ２１は、このデータを受信した場合は、カウンタパーツ２１自身を振動／音／点滅等させて当該電子マネーカード１０保有者に警告する。これにより、落したことに気がつかずに歩きつづけている保有者は電子マネーカード１０を落したことに即時に気がつき、落下等による紛失を免れることができる。

【００８６】（３）ケース３＜落下衝撃が規定以下＞

①電子マネーカード１０自身は、カウンタパーツ２１からの存在確認問合せが規定時間内にあるか否かを常時監視している。したがって、カウンタパーツ２１から発信する存在確認問合せが電子マネーカード１０に届かなくなった後で、この規定時間を経過したら電子マネーカード１０から存在確認自発発信のデータが発信される。電子マネーカード１０が発信する存在確認自発発信の電波出力はカウンタパーツ２１からの存在確認問合せ電波の出力よりも出力が大きいため、この場合はカウンタパーツ２１は存在確認自発発信のデータを受信することになる。この受信により、カウンタパーツ２１はカウンタパーツ２１自身を振動／音／点滅等させて電子マネーカード１０に警告する。

【００８７】②カウンタパーツ２１は、受信した存在確認応答の電波の強度（受信電界強度）により、カウンタパーツ２１と電子マネーカード１０との距離を計測している。この計測距離が規定距離より大きくなった場合、カウンタパーツ２１は、カウンタパーツ２１自身を振動／音／点滅等させて電子マネーカード１０保有者に警告する。さらに、カウンタパーツ２１が電子マネーカード１０から送出される方位／距離データに基づいてそれを表示し、また電子マネーカード１０に近づく程、振動／音／点滅等を強める。

【００８８】（４）ケース４＜置忘れたが存在確認問合せが電子マネーカード１０に届く＞

①距離を測定しているので、「落下衝撃が規定以下」の②の場合と同じである。

【００８９】（５）ケース５＜存在確認問合せは届かないが電子マネーカード１０からの存在確認自発発信がカウンタパーツ２に届く＞

この場合は、ケース３＜落下衝撃が規定以下＞と同じである。

【００９０】（６）ケース６＜電子マネーカード１０からの存在確認自発発信がカウンタパーツ２１に届かない＞

この場合は、電子マネーカード１０の保有者はカウンタパーツ２を頼りに心当りを捜すことになる。

【００９１】なお、カウンタパーツ２１の捜索ボタン２１９を押下することにより、電子マネーカード１０の発信する存在確認自発発信をカウンタパーツ２１が受信した場合は、カウンタパーツ２１が電子マネーカード１０から送出される方位／距離データに基づいてそれを表示し、また電子マネーカード１０に近づく程、振動／音／点滅等を強めることができる。

【００９２】（７）ケース７＜紛失＞

捜索しても見つからないまたはカウンタパーツ２１の警告に気づかなかった場合等、すなわち紛失した場合は、緊急パーツ２２を使用して紛失盗難センタ２４に届けることになる。

【００９３】（８）ケース８＜盗難＞

この場合は、ケース７「紛失」と同じである。

【００９４】以下に、ケース７「紛失」とケース８「盗難」の場合についてのシステムの動作について説明する。なお、これらの場合のシステムの動作は同一である。

【００９５】電子マネーカード１０の紛失盗難にあった場合は、電子マネーカード１０の保有者は緊急パーツ２２を使用する。緊急パーツ２２には、あらかじめ、１または複数の電子マネーカード１０の電子マネーカードＩＤ及び紛失盗難センタ２４の電話番号等が設定されている。これを近くの電話機または緊急受付装置２３の緊急パーツ２２挿入スロットに挿入する。緊急パーツ２２を電話機に挿入した場合は、その電話機は挿入された緊急パーツ２２に登録されている１または複数の電子マネーカードＩＤを電話機の表示部に表示する。緊急パーツ２２を電話機に挿入した人は、表示された電子マネーカードＩＤの中から紛失盗難にあった電子マネーカード１０の電子マネーカードＩＤを選択する。選択された電子マネーカードＩＤが紛失盗難のあった電子マネーカード１０の電子マネーカードＩＤとなり、自動的に紛失盗難センタ２４へ送出される。

【００９６】緊急パーツ２２を緊急受付装置２３に挿入することもできる。この場合の緊急受付装置２３の動作は電話機の動作と同一である。

【００９７】なお、緊急パーツ２２に登録されている電子マネーカードＩＤが１つしかない場合は、この電子マネーカードＩＤが紛失盗難のあった電子マネーカード１０の電子マネーカードＩＤとなる。

【００９８】緊急パーツ２２が挿入された電話機または緊急受付装置２３は、このようにして決定した電子マネーカードＩＤを紛失盗難センタ２４へ送信する。

【００９９】なお、緊急受付装置２３は、金融機関の本支店，郵便局，警察署，交番，駅，病院，公共施設等に設置されている。

【０１００】緊急受付装置２３から電子マネーカードＩＤを受信した紛失盗難センタ２４は、受信した電子マネーカードＩＤを紛失盗難データベースに登録するとともに、人工衛星２５に対して電子マネーカードＩＤを送信

する。

【０１０１】人工衛星２５は、紛失盗難センタ２４から送信された電子マネーカードＩＤを受し、受信した電子マネーカードＩＤをもつ電子マネーカード１０をＳＯＳ発信電子マネーカード１０に指定し、ＳＯＳ発信指示をブロードキャストする。

【０１０２】人工衛星２５からこのＳＯＳブロードキャストを受信した電子マネーカード１０は、ブロードキャストされている電子マネーカードＩＤが自電子マネーカード１０の電子マネーカードＩＤでない場合、このブロードキャストを無視する。

【０１０３】しかし、ブロードキャストされている電子マネーカードＩＤが自電子マネーカード１０の電子マネーカードＩＤである場合(以降、この電子マネーカード１０をカードＳとする)、カードＳは自身の取引機能停止を行う。そして、ビニールチューブ等でカードＳに繋がっている内蔵の風船を外部に放出し、内蔵のガスを注入して膨らませる。これによって、カードＳが何かに引っ掛っていなければ水空中に浮び、空中からブロードキャストすることになる。

【０１０４】もし、カードＳが何かに引っ掛っていて水空中に浮揚できないときでも、ＳＯＳがブロードキャストされる。なお、ＳＯＳのブロードキャストは、次の機器に対して行われる。

【０１０５】ａ．カードＳの電子マネーカードＩＤと特定の関係にある電子マネーカードＩＤをもつ電子マネーカード１０(以降、カードＲとする)

ｂ．緊急受付装置２３

ｃ．紛失盗難センタ２４

カードＳからのＳＯＳを受信した１または複数の上記機器は、カードＳからブロードキャストされたＳＯＳを受信し、そのＳＯＳを自機器に取込む。

【０１０６】以下に、ＳＯＳを取込んだ電子マネーカード１０(カードＲ)の動作について説明する。

【０１０７】カードＲは、カードＲの電子マネーカードＩＤによりＳＯＳ受信の旨をカードＲの保有者に知らせる報告時期、例えばＳＯＳ受信日から「何日後」を計算する。そして、ＳＯＳ受信の報告日になったら、振動／音／点滅等により、ＳＯＳ受信の旨をカードＲの保有者に知らせる。

【０１０８】これを知ったカードＲの保有者は、報告日からの定期間内に、近くの電話機または金融機関本支店，郵便局，警察署，交番，駅，病院，公共施設等に設置されている緊急受付装置２３とカードＲとを通信させることによって、カードＲが保持しているＳＯＳを緊急受付装置２３経由で紛失盗難センタ２４に送信する。

【０１０９】紛失盗難センタ２４は、緊急受付装置２３経由で回収したＳＯＳから紛失盗難のあった電子マネーカード１０(カードＳ)の電子マネーカードＩＤを知り、このカードＳの事件が解決しているか否かを自センタ２４に保持している解決データベースを調査する。調査の結果、解決データベースに登録されていなかったら、事件が解決したとして解決データベースの登録内容を抹消する。

【０１１０】次に、紛失盗難センタ２４は、カードＳのＳＯＳのブロードキャストを停止させるべく、カードＳの電子マネーカードＩＤを人工衛星２５に送信する。

【０１１１】次に、紛失盗難センタ２４は、カードＳのＳＯＳをカードＳを発行した金融機関２６に送信する。ＳＯＳの送信を受けた金融機関２６は、カードＳの電子マネーカードＩＤから、カードＳの発行を受けたときに登録した名義人あるいはその後の届けのあった変更名義人に対し、カードＳの電子マネー等を回収したことを連絡する。当然ながら、回収したＳＯＳにはカードＳがＳＯＳをブロードキャストしたときにカードＳが保有していた金額の電子マネー及びその他のデータすべてが含まれている。

【０１１２】人工衛星２５は、紛失盗難センタ２４から指示されたカードＳに対してＳＯＳ停止指示をブロードキャストする。なお、ＳＯＳ停止指示のブロードキャストを受信して何らかの動作をする機器は、カードＳとカードＲである。

【０１１３】カードＳは、この停止指示を受信したらＳＯＳのブロードキャストを停止し、風船を切離す。また、存在確認自発発信を行う。

【０１１４】カードＲについては、カードＲがカードＳの電子マネーカードＩＤをもつＳＯＳを保持しているカードＲである場合は、カードＳの電子マネーカードＩＤをもつＳＯＳを廃棄する。したがって、カードＳからのＳＯＳを受信したカードＲの中には、自カードＲの保有者への報告前にＳＯＳを廃棄する場合もあるため、カードＲの保有者がまったく知らない間に、自分の保持しているカードＲがＳＯＳを受信し廃棄していることもある。

【０１１５】なお、個人が保持する電子マネーカード１０と取引をする店舗機２０は、取引相手である個人保持の電子マネーカード１０がＳＯＳデータを保持しているカードＲである場合は、カードＲの保有者へのＳＯＳ保持報告前であっても、カードＲが保持している複数のカードＳのＳＯＳを電子マネーカード１０から取込んで、取込んだＳＯＳを紛失盗難センタ２４に送信できる機能を持っている。すなわち、店舗機２０は緊急受付装置２３の代行機能も持っている。

【０１１６】また、このようにしてＳＯＳを取込まれた電子マネーカード１０は、自身が保持しているすべてのＳＯＳを廃棄する。

【０１１７】次に、電子マネーカード１０の正当な保有者でない者の使用の防止についての対策を、図７および図８を参照して説明する。

【０１１８】＜２４ｈ有効パスワード＞図７に示すよう

に、パスワードとして真偽混合のパスワードを必要個数ユーザが設定する。ここで、Pt１～Ptnは真のパスワードであり、Pf１～Pfmは偽のパスワードである。

【０１１９】ここでのパスワード設定の仕方は、真のパスワードだけを入力するのではなく、故意に、偽のパスワード入力も必要とすることを特徴とする。しかも、パスワードは曜日の違いまたは日にちの違いにより、入力する真のパスワード数と偽のパスワード数が違うことを特徴とする。

【０１２０】この方法を図７を使用して説明する。当日の最初の使用前にパスワードを入力しないと電子マネーカード１０は一時的機能停止状態となっている。まず、パスワードの入力にあたっては、当該電子マネーカード１０に登録されている真偽混合のパスワードすべてを当該電子マネーカード１０に備付けの表示装置に表示する。当該電子マネーカード１０の保有者は、表示された真偽混合のパスワードから次のようにして入力するパスワードを選択する。また、パスワードの選択による入力にあたっては、電子マネーカード１０はパスワードを１ケ選択されるごとに「次は？」というような質問はせずにノーアクションのままである。すなわち、これでパスワードの入力が終了なのかまたは引続いてパスワードを入力するのかは、パスワードの入力者に委ねる。そして、パスワード入力終了の宣言の結果、入力されたパスワードが当日のパスワードと違っていれば、単に「パスワード誤り」を表示する。この「パスワード誤り」が連続して規定の回数に達した場合は、規定の日数の使用を停止する。

【０１２１】次に、パスワードの具体的な入力の仕方について述べる。当日が日曜日である場合は、この日の最初の使用前にパスワードを入力するが、日曜日であるので入力するパスワードは、任意の真のパスワードが１ケと任意の偽のパスワードが３ケである。これにより、日曜日当日における電子マネーカード１０の使用が可能となる。そして、このパスワードは、翌日午前０時を期して無効となる。すなわち、翌日の月曜日午前０時からは、あらためて任意の真のパスワードを２ケと任意の偽のパスワードを２ケ入力しないと、翌日の月曜日には電子マネーカード１０の使用ができなくなる。

【０１２２】図８においても同様である。図７と図８の違いは、パスワードを曜日で変更するか日にちで変更するかの違いだけである。

【０１２３】これにより、電子マネーカード１０を盗んだ人が、正当な保有者の属性を調査してパスワードを類推したとしても、他のパスワードの入力方法と同様に真のパスワードを１ケ選択する可能性が高いため、電子マネーカード１０の正当な保有者でない者の使用を高い確率で防止できる。

【０１２４】また、盗難者がパスワードの入力無しに盗んだ電子マネーカード１０を使用できるのは、電子マネーカード１０がカウンタパーツ２１とともに盗まれて、かつ盗難のあった電子マネーカード１０に対する人工衛星２５からの機能停止指示が盗難当日の盗難者の使用に間に合わなかった場合だけである。しかも、盗難当日だけである。

【０１２５】また、電子マネーカード１０は１日に使用できる金額の限度額をプリセット値として設定でき、一時的にこれを増額することもできる。さらに、１日の使用限度額を増額した場合でも、規定の時間経過後は元のプリセット値に戻る。

【０１２６】したがって、電子マネーカード１０の機能活性化用のパスワード方法と、１日の使用限度額増額用のパスワード方法の２種類のパスワード方法を使用することにより、盗難による被害金額をさらに少なくすることができる。

【０１２７】また、パスワードの中に本人の属性（例えば、誕生日、電話番号、部屋番号など）を含ませると、その本人の身辺を調査することによってパスワードが推定できてしまう。そこで、パスワードの中に、カード所有者の嘘の属性を故意に含ませることによって、パスワードの推定が困難になり、不正使用防止効果をさらに向上させることができる。

【０１２８】図９は、カウンタパーツ２１から電子マネーカード１０へ送信する存在確認問合せ４０のデータ内容であり、電子マネーカードＩＤ４１と問合せコード４２からなる。

【０１２９】電子マネーカードＩＤ４１は、電子マネーカード１０と当該電子マネーカード１０のカウンタパーツ２１を特定するものであり、システムにおいてユニークである。問合せコード４２はカウンタパーツ２１から電子マネーカード１０への存在確認問合せを示すコードである。

【０１３０】電子マネーカードＩＤ４１は、当該電子マネーカード１０を発行した発行金融機関２６の支店を示す発行金融機関支店コード４１３と、発行金融機関支店の属する発行金融機関２６を示す発行金融機関コード４１２と、発行金融機関２６の属する国を示す国コード４１１と、その他のデータであるその他４１４とからなる。

【０１３１】図１０は、電子マネーカード１０への存在確認問合せに対する電子マネーカード１０からカウンタパーツ２１へ送信する存在確認応答５０のデータ内容である。

【０１３２】電子マネーカードＩＤ５１は、電子マネーカードＩＤ４１と同一のＩＤである。経緯度５２は、電子マネーカード１０がＧＰＳシステム（人工衛星による位置確認システム）から受信した電子マネーカード１０の現在位置を示す経緯度情報である。発信時刻５３は、電子マネーカード１０が存在確認応答５０を送信した時の時刻であり、時分秒およびマイクロセコンドまでの情

報が格納されている。応答コード５４は、カウンタパーツ２１からの存在確認問合せに対する電子マネーカード１０からの応答データであることを示す。

【０１３３】図１２は、電子マネーカード１０からカウンタパーツ２１へ送信する存在確認自発発信６０のデータ内容であり、電子マネーカードＩＤ６１は電子マネーカードＩＤ４１と同一のものである。経緯度６２は、経緯度５２と同一の意味の情報である。発信時刻６３は、発信時刻５３と同一の意味の情報である。自発発信コード６４は、カウンタパーツ２１からの存在確認問合せなしに、電子マネーカード１０から一方的に送信した存在確認であることを示す。

【０１３４】図１３は、カウンタパーツ２１から電子マネーカード１０への存在確認問合せの停止を連絡するために電子マネーカード１０へ送信する機能停止７０のデータ内容である。電子マネーカードＩＤ７１は、電子マネーカードＩＤ４１と同一のものである。機能停止時間７２は、存在確認問合せを停止する時間間隔を示すものである。機能停止コード７３は機能停止を示すものである。

【０１３５】図１４は、電子マネーカード１０の機能停止のクラス分けと他機との取引機能を示す図であり、機能停止のクラスとしては、第１級から第３級までがあり、いずれのクラスにおいても緊急受付装置２３との取引または交信は可能になっている。しかし、第１級の機能停止モードでは、店舗機２０との取り引きが禁止される。また、第１級および第２級の機能停止モードでは、パスワードの入力が禁止される。

【０１３６】電子マネーカード１０は、電源オンスイッチを短時間押下すると電源オンとなり、長時間押下すると、電源オンで、かつ緊急受付装置２３のみとの取引または交信が可能になる。さらに、電源オン中に、電源オンスイッチを長時間押下しても、緊急受付装置２３のみとの取引または交信が可能になる。

【０１３７】図１５は、紛失盗難センタ２４から人工衛星２５へ送信するＳＯＳ発信指示８０のデータ内容である。人工衛星ＩＤ８１は、ＳＯＳ発信指示８０を受信する人工衛星２５を特定するコードである。ＳＯＳ発信指示コード８２は、人工衛星２５に対して指示内容であり、紛失盗難にあった電子マネーカードＩＤ８３の電子マネーカード１０に対してＳＯＳ発信指示のブロードキャストを指示する内容である。電子マネーカードＩＤ８３は、紛失盗難にあったと届けがなされて受付けた電子マネーカード１０の電子マネーカードＩＤである。

【０１３８】図１６は人工衛星２５から紛失盗難にあった電子マネーカードＩＤ８３の電子マネーカード１０に対してＳＯＳ発信指示をブロードキャストするＳＯＳ発信指示ブロードキャスト９０のデータ内容である。ＳＯＳ発信指示コード９１は、このブロードキャストがＳＯＳ発信指示であることを示している。電子マネーカードＩＤ９２は、このＩＤを持つ電子マネーカード１０に対するＳＯＳ発信指示であることを示す。

【０１３９】図１７は、紛失盗難センタ２４から人工衛星２５へ送信するＳＯＳ停止指示１００のデータ内容である。人工衛星ＩＤ１０１は、ＳＯＳ停止指示１００を受信する人工衛星２５を特定するコードである。ＳＯＳ停止指示コード１０２は、人工衛星２５に対しての指示内容であり、電子マネーカードＩＤ１０３の電子マネーカード１０に対してＳＯＳ停止指示のブロードキャストを指示する内容である。

【０１４０】図１８は、人工衛星２５から電子マネーカードＩＤ１５２の電子マネーカード１０に対してＳＯＳ停止指示をブロードキャストするＳＯＳ停止指示ブロードキャスト１５０のデータ内容である。ＳＯＳ停止指示コード１５１は、このブロードキャストがＳＯＳ停止指示であることを示している。電子マネーカードＩＤ１５２は、このＩＤを持つは電子マネーカード１０に対するＳＯＳ停止指示であることを示す。

【０１４１】図１９は、人工衛星２５からのＳＯＳ発信指示ブロードキャスト９０でＳＯＳ発信を指示された電子マネーカードＩＤ９２(＝電子マネーカードＩＤ１６２)の電子マネーカード１がブロードキャストするＳＯＳ１６０のデータ内容である。ＳＯＳコード１６１は、このブロードキャストがＳＯＳであることを示している。電子マネーカードＩＤ１６２は、ＳＯＳをブロードキャストしている電子マネーカード１０の電子マネーカードＩＤである。経緯度１６３は、当該電子マネーカード１０がＧＰＳシステムから受信した電子マネーカード１０の現在位置を示す経緯度情報である。発信時刻１６４は、電子マネーカード１０がＳＯＳをブロードキャストした時の時刻であり、時分秒およびマイクロセコンドまでの情報が格納されている。格納電子マネー１６５は、当該電子マネーカード１０が格納している電子マネーを暗号化したものである。その他格納データ１６６は当該電子マネーカード１０が格納している電子マネー１６５以外の格納データを暗号化したものである。

【０１４２】図２０は、緊急パーツ２２のデータ内容である。１７１は付加機能用のデータである。電子マネーカードＩＤ１７２は電子マネーカードＩＤであり、複数個の電子マネーカードＩＤを格納できる。緊急受付装置電話番号１７３は緊急受付装置の電話番号である。

【０１４３】図１１は、カウンタパーツ２１から電子マネーカード１０に対する機能最下位のデータ内容であり、電子マネーカードＩＤ１８１、機能再開コード１８２で構成され、機能再開コード１８２の内容に応じて、第１級から第３級までの機能停止状態が解除される。

【０１４４】図２１は、電子マネーカード１０の紛失盗難防止に関わる基本動作を示すフローチャートである。

【０１４５】電子マネーカード１０は、本発明の目的のために使用する副電源と電子マネーカード１０本来の目

的のために使用する主電源とを備えている。

【０１４６】主電源がオンとなった時は、無条件に図３０のフローチャートに示す共通処理を実行する（ステップ２１０４）。そして、図３０に示す共通処理からリターンしてきたら図２１に示す主電源オン中の動作に移行する。

【０１４７】主電源オン中に、主電源オフ操作が行われた場合は、主電源をオフにする旨を表示／音声等により電子マネーカード１０の保有者に連絡した後、主電源をオフにし、終了する（ステップ２１０１～２１０３）。

【０１４８】主電源オン状態となった後は、事象待ち状態が解除される。そして、どの事象が発生したのかの切分けが行なわれる。

【０１４９】この切分けによって、
①緊急受入装置２３との取引、
②他機との取引／自機内の操作、
③衝撃検出、
④自マネーカードＩＤ受信、
⑤他マネーカードＩＤ受信、
⑥タイムアウト、
の発生事象が判明する（ステップ２１０５～２１１０）。

【０１５０】そして、この発生事象に対応した処理を実行する（ステップ２１１１～２１１６）。

【０１５１】以降、この発生事象ごとに個別に説明する。

【０１５２】（１）緊急受入装置４との取引である場合、図２２に示すように、図３０に示す共通処理を実行し、終了すなわち事象待ち状態となる（ステップ２２０１）。

【０１５３】（２）他機との取引／自機内の操作である場合、図３０に示す副動作を実行しし（ステップ２３０１）、共通処理からリターンしてきた場合は、図２３の詳細フローチャート示すように、目的の取引を実行する(ステップ２３０２)。次に、取引相手機が店舗機２０であるか否かをチェックする(ステップ２３０３)。

【０１５４】取引相手機が店舗機２０である場合は、自電子マネーカード１０がＳＯＳを保持しているか否かをチェックし(ステップ２３０４)、保持していれば保持している全ＳＯＳも取引相手機である店舗機２０に送信する(ステップ２３０５)。その後、保持しているＳＯＳを廃棄し(ステップ２３０６)、終了すなわち事象待ち状態となる。

【０１５５】ステップ２３０４のチェックで他電子マネーカード１のＳＯＳを保持していないと判明した場合は、そのまま終了すなわち事象待ち状態となる。

【０１５６】また、ステップ２３０３のチェックで取引相手機が店舗機２０でないと判明した場合は、そのまま終了すなわち事象待ち状態となる。

【０１５７】（３）衝撃検出、すなわち規定以上の衝撃があった場合は、図２４の詳細フローチャートに示すように自電子マネーカード１０の取引き機能を第３級取引機能停止とする(ステップ２４０１)。

【０１５８】第３級取引機能停止とは、自電子マネーカード１０の次のユーザ操作においてパスワードの入力を求める状態のことである。

【０１５９】次に、図１２に示した存在確認自発発信のデータ５０を発信する(ステップ２４０２)。その後、Ｔ１のタイマをセットし(ステップ２４０３)、終了すなわち事象待ち状態となる。

【０１６０】（４）自マネーカードＩＤの存在するデータを受信した場合は、図２５の詳細フローチャートに示すように、受信データがどのようなデータであるかを分析する。この分析の結果、受信データは、
①図９に示すカウンタパーツ２１からの存在確認問合せの受信データ４０（ステップ２５０１）、
②図１３に示すカウンタパーツ２１からの機能停止連絡の受信データ７０(ステップ２５０２)
③図２１に示すカウンタパーツ２１からの機能再開連絡の受信データ１８０(ステップ２５０３)、
④図１６に示す人工衛星２５からのＳＯＳ発信指示ブロードキャストの受信データ９０(ステップ２５０４)、
⑤図１８に示す人工衛星２５からのＳＯＳ停止指示ブロードキャストの受信データ１５０(ステップ２５０５)のように分けられる。

【０１６１】以降、この受信データごとに個別に説明していく。

【０１６２】まず、図９に示すカウンタパーツ２１からの存在確認問合せを受信した場合(ステップ２５０１)、Ｔ１およびＴ２のタイマをリセットする(ステップ２５０６)。そして、自電子マネーカード１０が存在確認自発発信中か否かをチェックする(ステップ２５０７)。存在確認自発発信中であれば、図１２に示す存在確認自発発信６０を発信する(ステップ２５０８)。その後、タイマＴ１をセットし(ステップ２５０９)、終了すなわち事象待ち状態となる。

【０１６３】ステップ２５０７０のチェックの結果、自電子マネーカード１０が存在確認自発発信中でなければ、図１０に示す存在確認応答発信５０を発信する(ステップ２５１０)。その後、図１０に示す存在確認応答データ５０を発信する(ステップ２５１３)。次に、タイマＴ２をセットし(ステップ２５１１)、終了すなわち事象待ち状態となる。

【０１６４】次に、カウンタパーツ２１から図１３に示す機能停止データ７０を受信した場合(ステップ２５０２)、自電子マネーカード１０の取引き機能を第３級取引機能停止とする(ステップ２５１２)。そして、機能停止時間とされた機能停止データ７０中の機能停止時間７２をタイマＴ３としてセットし(ステップ２５１４)、終了すなわち事象待ち状態となる。

【０１６５】次に、カウンタパーツ２１から図１１に示す機能再開データ１８０を受信した場合は(ステップ２５０３)、タイマＴ３をリセットし(ステップ２５１５)、第３級取引機能停止の解除を行なう(ステップ２５１６)。その後、図１０に示す存在確認応答データ５０を発信する(ステップ２５１６)。次に、タイマＴ２をセットし(ステップ２５１８)、終了すなわち事象待ち状態となる。

【０１６６】次に、図１６に示す人工衛星２５からのＳＯＳ発信指示ブロードキャストデータ９０を受信した場合は(ステップ２５０４)、自電子マネーカード１０の取引機能を第１級取引機能停止とする(ステップ２５１９)。次に、自電子マネーカード１０に内蔵している風船を放出し(ステップ２５２０)、その放出した風船にやはり内蔵しているガスを注入する(ステップ２５２１)。そして、自電子マネーカード１０の表示装置に「電子マネーカード１０を任意の金融機関２６へ届けて下さい」の意味の表示をする(ステップ２５２２)。

【０１６７】その後、自電子マネーカード１０に格納している電子マネーとその他のデータをそれぞれ異なる暗号化方法により暗号化し(ステップ２５２３)、図１９に示すＳＯＳデータ１６０を発信する(ステップ２５２４)。その後、タイマＴ４をセットし(ステップ２５２５)、終了すなわち事象待ち状態となる。

【０１６８】次に、図１８に示す人工衛星２５からのＳＯＳ停止指示ブロードキャストデータ１５０を受信した場合は(ステップ２５０５)、自電子マネーカード１０に格納している電子マネーとその他のデータを廃棄する(ステップ２５２６)。そして、自電子マネーカード１０の取引機能を第１級取引機能停止とし(ステップ２５２７)、ＳＯＳデータ１６０の発信を停止する(ステップ２５２８)。

【０１６９】その後、自電子マネーカード１０の表示装置に「電子マネーカード１０を任意の金融機関２６へ届けて下さい」の意味の表示をする(ステップ２５２９)。そして、放出している風船を自電子マネーカード１０から切離し(ステップ２５３０)、図１２に示す存在確認自発発信データ６０を発信する(ステップ２５３１)。その後、タイマＴ５をセットし(ステップ２５３２)、終了すなわち事象待ち状態となる。

【０１７０】次に、他のマネーカードＩＤの存在するデータを受信した場合、図２７の詳細フローチャートに示すように、その受信データがどのようなデータであるかを分析する。この分析の結果、受信データは、

①図１９に示すＳＯＳデータ１６０(ステップ７０１)、

②図１８に示す人工衛星２５からのＳＯＳ停止指示ブロードキャストデータ１５０(ステップ２７０２)、

のように分けられる。

【０１７１】以降、この受信データごとに個別に説明していく。

【０１７２】まず、図１９に示すＳＯＳデータ１６０を受信した場合は(ステップ２７０１)、受信データ中の電子マネーカードＩＤ１６２と同一ＩＤの電子マネーカード１０のＳＯＳデータ１６０をすでに保持しているかチェックする(ステップ２７０３)。このチェックの結果、保持していなければ、ＳＯＳデータ１６０のデータをそっくりそのまま自電子マネーカード１０に格納する(ステップ２７０４)。その後、自電子マネーカード１０の電子マネーカードＩＤに基づいて自電子マネーカード１０の保有者にＳＯＳデータ１６０のデータ保持を報告すべき時期を計算し(ステップ２７０５)、計算した結果の報告時期をタイマＴ６に格納しておく(ステップ２７０６)。そして、終了すなわち事象待ち状態となる。

【０１７３】ステップ２７０３でのチェックの結果、すでに保持していれば何もせずに終了すなわち事象待ち状態となる。

【０１７４】次に、図１８に示す人工衛星２５からのＳＯＳ停止指示ブロードキャストデータ１５０を受信した場合は(ステップ２７０２)、受信データ中の電子マネーカードＩＤ１５２と同一ＩＤの電子マネーカード１０のＳＯＳデータ１６０を保持しているか否かをチェックする(ステップ２７０７)。このチェックの結果、保持していれば、保持している当該ＳＯＳデータ１６０のデータを廃棄する(ステップ２７０８)。その後、自電子マネーカード１０の表示装置に「自電子マネーカード１０には他の自電子マネーカード１０のデータが保持されていますので緊急受付装置２３を使用して〇年〇月〇日までに届けて下さい」の意味の表示、すなわちＳＯＳ届け勧告中の場合は(ステップ２７０９)、このＳＯＳ届け勧告が受信データ中の電子マネーカードＩＤ１６２の電子マネーカード１０のＳＯＳデータ１６０によるものか否かをチェックする(ステップ２７１０)。そうであれば、ＳＯＳ届け勧告を停止し(ステップ２７１１)、終了すなわち事象待ち状態となる。

【０１７５】ステップ２７０７でのチェックの結果、そうでなければ何もせずに終了すなわち事象待ち状態となる。

【０１７６】ステップ２７０８での保持しているＳＯＳデータ１６０のデータを廃棄後、ＳＯＳデータ１６０のデータの届けが指定の期限までになされていない場合は(ステップ２７１２)、その無届けが今受信したＳＯＳ停止指示ブロードキャストデータ１５０の電子マネーカードＩＤ１５２と同一ＩＤの電子マネーカード１０の無届けか否かをチェックする(ステップ２７１３)。このチェックの結果、そうであれば第２級取引機能停止を解除し(ステップ２７１４)、第３級取引機能停止とする(ステップ２７１５)。その後、「主電源オフ指示」を行って(ステップ２７１６)主電源オフ時動作へ分岐する。

【０１７７】ステップ２７１３でのチェックの結果、そうでなければ、終了すなわち事象待ち状態となる。

【０１７８】次に、タイムアウトの事象を検出した場合は(ステップ２１００)、図２８の詳細フローチャートに示すように、さらにその事象がどのタイムアウト事象かを分析する。

【０１７９】この分析の結果、タイムアウト事象は、
①衝撃によるタイマＴ１のタイムアウト(ステップ２８０１)、
②カウンタパーツ２１からの無問合せ等のタイマＴ２のタイムアウト(ステップ２８０２)、
③機能再開連絡なしのタイマＴ３のタイムアウト(ステップ２８０３)、
④ＳＯＳ発信中のタイマＴ４のタイムアウト(ステップ２８０４)、
⑤ＳＯＳ停止後のタイマＴ５のタイムアウト(ステップ２８０５)
⑥ＳＯＳ届け勧告日到来のタイマＴ６タイムアウト(ステップ２８０６)、
⑦ＳＯＳ届け勧告期限切れのタイマＴ７のタイムアウト(ステップ２８０７)のように分けられる。

【０１８０】以降、このタイムアウト事象ごとに個別に説明していく。

【０１８１】衝撃によるタイマＴ１のタイムアウトの場合は(ステップ２８０１)、第３級取引機能停止とする(ステップ２８０８)。そして、図１２に示す存在確認自発発信データ６０を発信する(ステップ２８０９)。その後、タイマＴ１をセットし(ステップ２８１０)、終了すなわち事象待ち状態となる。

【０１８２】カウンタパーツ２１からの無問合せ等のタイマＴ２のタイムアウトの場合は(ステップ２８０２)、第３級取引機能停止とする(ステップ２８１１)。そして、図１２に示す存在確認自発発信データ６０を発信する(ステップ２８１２)。その後、タイマＴ２をセットし(ステップ２８１３)、終了すなわち事象待ち状態となる。

【０１８３】機能再開連絡なしのタイマＴ３のタイムアウトの場合は(ステップ２８０３)、第３級取引機能停止とする(ステップ２８１４)。そして、図１２に示す存在確認自発発信データ６０を発信する(ステップ２８１５)。その後、タイマＴ２をセットし(ステップ２８１６)、終了すなわち事象待ち状態となる。

【０１８４】ＳＯＳ発信中のタイマＴ４のタイムアウトの場合は(ステップ２８０４)、第１級取引機能停止とする(ステップ２８１７)。そして、図１９に示すＳＯＳデータ１６０を発信する(ステップ２８１８)。その後、タイマＴ４をセットし(ステップ２８１９)、終了すなわち事象待ち状態となる。

【０１８５】ＳＯＳ停止後のタイマＴ５のタイムアウトの場合は(ステップ２８０５)、第１級取引機能停止とする(ステップ２８２０)。そして、図１２に示す存在確認自発発信データ６０を発信する(ステップ２８２１)。その後、タイマＴ２をセットし(ステップ２８２２)、終了すなわち事象待ち状態となる。

【０１８６】ＳＯＳ届け勧告日到来のタイマＴ６タイムアウトの場合は(ステップ２８０６)、自電子マネーカード１０の表示装置に「自電子マネーカード１０には他の自電子マネーカード１０のデータが保持されていますので緊急受付装置２３を利用して○年○月○日までに届けて下さい」の意味の表示、すなわちＳＯＳ届け勧告をする(ステップ２８２３)。その後、届け期限日を自電子マネーカードＩＤに基づいて算出してそれをタイマＴ７としてセットし(ステップ２８２４)、終了すなわち事象待ち状態となる。

【０１８７】ＳＯＳ届け勧告期限切れのタイマＴ７のタイムアウトの場合は(ステップ２８０７)、第２級取引機能停止とする(ステップ２８２５)。そして、自電子マネーカード１０の表示装置に「自電子マネーカード１０には他の自電子マネーカード１０のデータが保持されていますが、○年○月○日までの期限内に届けがされませんでしたので、本電子マネーカード１０は第２級取引機能停止としました。できるだけ早く緊急受付装置４を利用して届けて下さい」の意味の表示、すなわちＳＯＳ届け期限切れ兼届け勧告をする(ステップ２８２６)。そして、終了すなわち事象待ち状態となる。

【０１８８】次に、電子マネーカード１０の各処理から呼出されて処理を行なう共通処理について図３０および図３１のフローチャートを使用して説明する。

【０１８９】電子マネーカード１０の各処理から呼出されて共通処理を行なう場合は、電子マネーカード１０の状態がどのような状態であるか、またはどのような取引要求であるか等を分析する。この分析の結果、本共通処理では、
①第１級取引機能停止の状態(ステップ３００１)、
②第２級取引機能停止の状態(ステップ３００２)、
③第３級取引機能停止の状態(ステップ３００３)、
④緊急受付装置２３との取引き要求(ステップ３００４)、
⑤その他(ステップ３００５)、
のように分けられる。

【０１９０】以降、この状態ごとに個別に説明していく。

【０１９１】まず、第１級取引機能停止の状態の場合は(ステップ３００１)、本電子マネーカード１０の表示装置に「本電子マネーカード１０を最寄りの金融機関に持参して下さい」の意味の表示、すなわち金融機関２６への持参勧告をし(ステップ３００６０)、主電源をオフすべく「主電源オフ指示」を行う(ステップ３００７)。

【０１９２】次に、第２級取引機能停止の状態の場合は(ステップ３００２)、緊急受付装置２３との取引き要求か否かをチェックする(ステップ３００８)。緊急受付装置２３との取引き要求であれば、緊急受付装置２３との

セションを開設し(ステップ３００９)、当該電子マネーカード１０が保持中の全ＳＯＳデータを緊急受付装置２３へ送信し(ステップ３０１０)、送信し終ったら緊急受付装置２３とのセションを解放する(ステップ３０１１)。次に、保持中の全ＳＯＳデータを廃棄し(ステップ３０１２)、第２級取引機能停止の解除を行い(ステップ３０１３)、第３級取引機能停止とする(ステップ３０１４)。そして、主電源をオフすべく「主電源オフ指示」を行う(ステップ３０１５)。

【０１９３】ステップ３００８での緊急受付装置２３との取引き要求か否かのチェックにおいて、緊急受付装置２３との取引き要求でない場合は、自電子マネーカード１０の表示装置に「自電子マネーカード１０には他の自電子マネーカード１０のデータが保持されていますが、○年○月○日までの期限内に届けがされませんでしたので、本電子マネーカード１０は第２級取引機能停止となっています。できるだけ早く緊急受付装置２３を使用して届けて下さい」の意味の表示、すなわちＳＯＳ届け期限切れ兼届け勧告をする(ステップ３０１６)。そして、呼出し元にリターンする。

【０１９４】次に、第３級取引機能停止の状態の場合は(ステップ３００３)、パスワードの入力を要求する(ステップ３０１７)。そして、入力されたパスワードが規定のパスワードであるか否かをチェックし(ステップ３０１８)、規定のパスワードである場合は第３級取引機能停止を解除し(ステップ３０２２)、呼出し元にリターンする。

【０１９５】しかし、入力されたパスワードが規定のパスワードでない場合は、連続して誤った回数をカウントし、このカウントが規定の回数に達したか否かをチェックする(ステップ３０１９)。チェックの結果、連続誤り回数が規定回数に達している場合は、第１級取引機能停止とする(ステップ３０２０)。そして、主電源をオフすべく「主電源オフ指示」を行う。

【０１９６】ステップ３０１９でのチェックの結果、連続誤り回数が規定回数に達していない場合は、再度パスワードを要求すべくステップ３０１８へ戻る。

【０１９７】次に、緊急受付装置２３との取引き要求の場合は(ステップ３００４)、緊急受付装置２３とのセションを開設し(ステップ３０２３)、当該電子マネーカード１０が保持中の全ＳＯＳデータを緊急受付装置２３へ送信し(ステップ３０２４)、送信し終ったら緊急受付装置２３とのセションを解放する(ステップ３０２５)。次に、保持中の全ＳＯＳデータを廃棄し(ステップ３０２６)、主電源をオフすべく「主電源オフ指示」を行う(ステップ３０２７)。

【０１９８】その他の場合は(ステップ３００５)、「主電源オン操作」か否かをチェックし(ステップ３０２８)、そうであれば、「パスワード要求」のステップ３０１７」へ分岐し、そうでなかったら呼出し元へリターンする。

【０１９９】以上が電子マネーカード１０の紛失盗難防止機能に関する動作である。

【０２００】図３２～図３４は、カウンタパーツ２１の動作を示すフローチャートである。以下、カウンタパーツ２１の動作を以下に説明する。

【０２０１】なお、カウンタパーツ２１の電源は１電源であり、基本的には常時オン状態である。

【０２０２】カウンタパーツ２１の動作においては、事象待ち状態で待機しており、この待ち状態が解除されたときに動作を開始する。そして、どの事象が発生したのかの切分けが行なわれる。この切分けによって、

①電源オン(ステップ３２０１)、
②問合せに対する存在確認応答の受信(ステップ３２０２)、
③電子マネーカード１０の存在確認自発発信データ６０の受信(ステップ３２０３)、
④ユーザからの機能停止の要求(ステップ３２０４)、
⑤ユーザからの機能停止解除の要求(ステップ３２０５)、
⑥ユーザからの臨戦体制解除の要求(ステップ３２０６)、
⑦タイムアウト(ステップ３２０７～３２１１)、
⑧電源オフ、

の発生事象が判明する。

【０２０３】以降、この発生事象ごとに個別に説明していく。

【０２０４】まず、電源がオンされた場合は(ステップ３２０１)、図９に示す存在確認問合せ４０のデータを電子マネーカード１０に送信する(ステップ３２１２)。その後、タイマＴ１０をセットし(ステップ３２１３)、終了すなわち事象待ち状態となる。

【０２０５】次に、図１０に示す問合せに対する存在確認応答データ５０の受信の場合は(ステップ３２０２)、臨戦体制か否かをチェックする(ステップ３１２４)。臨戦体制であれば、存在確認問合せに対する応答データ５０受信の報告をカウンタパーツ２１の表示装置に「存在確認問合せに対する応答を受信」の意味の表示をする(ステップ３２１５)。なお、この表示は表示装置の表示面積が小さい場合は数字コードとしてもかまわない。また、表示装置を設けることができない場合は、音声、振動の回数等によって報告してもよい。その後、タイマＴ１１をセットし(ステップ３２１６)、終了すなわち事象待ち状態となる。

【０２０６】臨戦体制でなければ、タイマＴ９をセットし、またタイマＴ１０をリセットし(ステップ３２１７)、終了すなわち事象待ち状態となる。

【０２０７】次に、図１２に示す電子マネーカード１の存在確認自発発信データ６０の受信の場合は(ステップ３２０３)、タイマＴ９とタイマＴ１０をリセットし(ス

テップ３２１８)、カウンタパーツ２１の表示装置に「自発発信存在確認受信」の意味の表示し(ステップ３２１９)、次に図９に示す存在確認問合せデータ４０を電子マネーカード１０に送信する(ステップ３２２０)。そしてどちらのタイマをセットするかを決めるため、臨戦体制か否かをチェックする(ステップ３２２１)。

【０２０８】臨戦体制であれば、タイマＴ１１をセットし(ステップ３２２２)、終了すなわち事象待ち状態となる。

【０２０９】臨戦体制でなければ、タイマＴ１０をセットし(ステップ３２２３)、終了すなわち事象待ち状態となる。

【０２１０】次に、ユーザからの機能停止の要求の場合は(ステップ３２０４)、図１３に示す機能停止データ７０を電子マネーカード１０に送信する(ステップ３２２４)。そして、ユーザが設定した再開までの時間をＴ３としてタイマＴ３をセットし(ステップ３２２５)、タイマＴ９とタイマＴ１０をリセットし(ステップ３２２６)、終了すなわち事象待ち状態となる。

【０２１１】次に、ユーザからの機能停止解除の要求の場合は(ステップ３２０５)、念のため機能停止中か否かをチェックする(ステップ３２２７)。機能停止中であれば、図２１に示す機能再開データ１８０を電子マネーカード１０に送信する(ステップ３２２８)。その後、タイマＴ８をセットし(ステップ３２２９)、終了すなわち事象待ち状態となる。

【０２１２】機能停止中でなければ、何もせずに終了すなわち事象待ち状態となる。

【０２１３】次に、ユーザからの臨戦体制解除の要求の場合は(ステップ３２０６)、臨戦体制を解除し(ステップ３２３０)、その後、終了すなわち事象待ち状態となる。

【０２１４】タイムアウトの場合、Ｔ３，Ｔ８，Ｔ９，Ｔ１０，Ｔ１１の５種類がある。

【０２１５】❶機能停止の時間が終了し、機能を再開する時間になったことを知らせるタイマＴ３のタイムアウト(ステップ３２０７)、

❷機能再開連絡後、電子マネーカード１０からその応答を規定の時間内に受信できなかったことを知らせるタイマＴ８のタイムアウト(ステップ３２０８)、

❸電子マネーカード１０に対して存在確認の問合せをする時刻になったことを知らせるタイマＴ９のタイムアウト(ステップ３２０９)、

❹電子マネーカード１０への存在確認の問合せに対して、電子マネーカード１０からその応答を規定の時間内に受信できなかったことを知らせるタイマＴ１０のタイムアウト(ステップ３２１０)、

❺臨戦体制中において、電子マネーカード１０に対して存在確認の問合せをする時刻になったことを知らせるタイマＴ１１のタイムアウト(ステップ３２１１) のように分類される。

【０２１６】以降、このタイムアウトごとに個別に説明していく。

【０２１７】まず、機能停止の時間が終了し、機能を再開する時間になったことを知らせるタイマＴ３のタイムアウトの場合は(ステップ３２０７)、図２１に示す機能再開データ１５０を電子マネーカード１０に送信する(ステップ３２３１)。その後、タイマＴ８をセットし(ステップ３２３２)、終了すなわち事象待ち状態となる。

【０２１８】次に、機能再開連絡後、電子マネーカード１０からその応答を規定の時間内に受信できなかったことを知らせるタイマＴ８のタイムアウトの場合は(ステップ３２０８)、カウンタパーツ２１の表示装置に「電子マネーカード１０から機能再開連絡に対する応答なし」の意味の表示をし(ステップ３２３３)、臨戦体制とする(ステップ３２３４)。その後、終了すなわち事象待ち状態となる。

【０２１９】次に、電子マネーカード１０に対して存在確認の問合せをする時刻になったことを知らせるタイマＴ９のタイムアウトの場合は(ステップ３２０９)、図９に示す存在確認問合せデータ４０を電子マネーカード１０に送信する(ステップ３２３５)。その後、タイマＴ１０をセットし(ステップ３２３６)、終了すなわち事象待ち状態となる。

【０２２０】次に、電子マネーカード１０への存在確認の問合せに対して、電子マネーカード１０からその応答を規定の時間内に受信できなかったことを知らせるタイマＴ１０のタイムアウトの場合は(ステップ３２１０)、カウンタパーツ２１の表示装置に「存在確認の問合せに対して、電子マネーカード１０から応答なし」の意味の表示をし(ステップ３２３７)、臨戦体制とする(ステップ３２３８)。その後、終了すなわち事象待ち状態となる。

【０２２１】臨戦体制中において、電子マネーカード１０に対して存在確認の問合せをする時刻になったことを知らせるタイマＴ１１のタイムアウトの場合は(ステップ３２１１)、図９に示す存在確認問合せデータ４０を電子マネーカード１０に送信する(ステップ３２３９)。その後、タイマＴ１１をセットし(ステップ３２４０)、終了すなわち事象待ち状態となる。

【０２２２】最後に、電源オフの場合は、何もせずに終了する。

【０２２３】図３５は、緊急受付装置２３の動作をフローチャートである。図３５を使用して緊急受付装置２３の動作を以下に説明する。

【０２２４】緊急受付装置２３の動作においては、常時呼出信号の受信待ちの状態になっている。そして、呼出信号を受信した場合どの機器からの呼出しかの切分けが行なわれ、

①電話機からの呼出し(ステップ３５０１)、
②緊急パーツ２２の緊急受付装置２３への直接挿入による呼出し(ステップ３５０１)、
③電子マネーカード１０からの呼出し(ステップ３５０３)、
に切分けられる。

【０２２５】以降、この呼出しごとに個別に説明していく。

【０２２６】まず、電話機からの呼出しの場合は(ステップ３５０１)、電話機との間でセションを開設し(ステップ３５０４)、電話機からデータを受信し(ステップ３５０５)、受信し終ったら電話機とのセションを解放する(ステップ３５０６)。なお、受信データは、紛失盗難届けデータである紛失盗難電子マネーカードＩＤと紛失盗難電子マネーカード１０発信のＳＯＳとの２種類がある。

【０２２７】電話機との間のセションを解放した後、紛失盗難センタ２４を呼出して(ステップ３５０７)、紛失盗難センタ２４との間でセションを開設し(ステップ３５０８)、電話機から受信したデータを紛失盗難センタ２４に送信し(ステップ３５０９)、送信し終ったらセションを解放する(ステップ３５１０)。その後、終了すなわち呼出信号の受信待ち状態となる。

【０２２８】緊急パーツ２２の緊急受付装置２３への直接挿入による呼出しの場合は(ステップ３５０１)、緊急パーツ２２に１または複数登録されている電子マネーカードＩＤのすべてを緊急受付装置２３の表示装置に表示し、紛失盗難のあった電子マネーカード１０として届ける１つの電子マネーカードＩＤを決定する(ステップ３５１１)。その後、緊急パーツ２２を排出し(ステップ３５１２)、決定した電子マネーカードＩＤを送信データとして前述したステップ３５０７以降の動作を行う。

【０２２９】次に、電子マネーカード１０からの呼出しの場合は(ステップ３５０３)、当該電子マネーカード１０との間でセションを開設し(ステップ３５１３)、電子マネーカード１０からデータを受信し(ステップ３５１４)、受信し終ったら電子マネーカード１１とのセションを解放する(ステップ３５１５)。その後、電子マネーカード１０から受信したデータを送信データとして前述したステップ３５０７以降の動作を行う。

【０２３０】図３６および図３７は、紛失盗難センタ２４の動作を示すフローチャートである。図３６および図３７を使用して紛失盗難センタ２４の動作を以下に説明する。

【０２３１】紛失盗難センタ２４の動作においては、常時、緊急受付装置２３からの呼出信号の受信待ちの状態になっている。そして、呼出信号を受信した場合は（ステップ３６０１）、緊急受付装置２３との間でセションを開設し(ステップ３６０２)、緊急受付装置２３からデータを受信し(ステップ３６０３)、受信し終ったら緊急受付装置２３とのセションを解放する(ステップ３６０４)。その後、受信したデータの種別、すなわち、
①受信データが電子マネーカードＩＤである場合(ステップ３６０５)
②受信データがＳＯＳデータである場合(ステップ３６０６)のそれぞれの動作
を行う。

【０２３２】以降、この動作ごとに個別に説明していく。

【０２３３】まず、受信データが電子マネーカードＩＤである場合は、紛失盗難届けであるため(ステップ３６０５)、届けがなされているか、すなわち紛失盗難データベースに届けのあった電子マネーカードＩＤが登録されているか否かをチェックする(ステップ３６０７)。紛失盗難データベースに登録されていない場合は、この事件が解決しているか、すなわち解決データベースに届けのあった電子マネーカードＩＤが登録されているか否かをチェックする(ステップ３６０８)。紛失盗難データベースと解決データベースとの両方に登録されていない場合だけ、紛失盗難データベースに届けのあった電子マネーカードＩＤを登録する(ステップ３６０９)。そして、ステップ３６１０へ進む。

【０２３４】紛失盗難データベースには登録されていなくて解決データベースに登録されている場合は、本事件は解決しているため、終了すなわち緊急受付装置２３からの呼出信号受信待ち状態となる。

【０２３５】また、ステップ３６０７でのチェックにより紛失盗難データベースに登録されている場合は、すでにこの電子マネーカードＩＤの紛失盗難届けを受付けていることを意味するため、何もせずに終了、すなわち緊急受付装置２３からの呼出信号受信待ち状態となる。

【０２３６】次に、受信データが図１９に示すＳＯＳデータ１６０である場合、すなわちＳＯＳデータ１２０の届けの場合は(ステップ３６０６)、届けがされているかすなわち今届けのあったＳＯＳデータ１６０内の電子マネーカードＩＤ１６２が紛失盗難データベースに登録されているか否かをチェックする(ステップ３６１１)。紛失盗難データベースに登録されている場合は、届けのあったＳＯＳデータ１６０内の電子マネーカードＩＤ１６２関連の情報を紛失盗難データベースから削除し(ステップ３６１２)、届けのあったＳＯＳデータ１６０内の電子マネーカードＩＤ１６２関連の情報を解決データベースに登録する(ステップ３６１３)。そして、ステップ３６１０へ進む。

【０２３７】ステップ３６１１のチェックで紛失盗難データベースに登録されていないことが判明した場合は、さらに届けのあったＳＯＳデータ１６０内の電子マネーカードＩＤ１６２関連の情報が解決データベースに登録されているか否かをチェックする(ステップ３６１４)。解決データベースに登録されていない場合は、届

けのあったＳＯＳデータ１６０内の電子マネーカードＩＤ１６２関連の情報を解決データベースに登録し(ステップ３６１５)、ステップ３６１０へ進む。

【０２３８】このケースは、届けのあったＳＯＳデータ１６０を発信した電子マネーカード１０の保有者が当該電子マネーカード１０の紛失盗難に気付かないまま当該電子マネーカード１０がＳＯＳデータ１６０を発信し、これを受信した電子マネーカード１０が届けたものである。しかし、これはありえない。なぜなら、紛失盗難の届けがあって人工衛星２５からＳＯＳデータ発信指示が出され、これによってだけＳＯＳデータを発信するのだからである。しかし、念のためのフェールセーフ的処置である。

【０２３９】ステップ３６１４でのチェックの結果、解決データベースに登録されていることが判明した場合は、当該ＳＯＳデータ１６０はすでに届けがされている意味であるので、何もせずに終了、すなわち緊急受付装置２３からの呼出信号受信待ち状態となる。

【０２４０】次に、ステップ３６１０以降の紛失盗難センタ２４の動作を説明する。

【０２４１】まず、人工衛星２５との間でセッションを開設する(ステップ３６１０)。その後の動作には
①紛失盗難届けである場合、
②ＳＯＳ１２０の届け
である場合の２種類がある。

【０２４２】以降、この動作ごとに個別に説明していく。

【０２４３】まず、紛失盗難届けである場合は(ステップ３６１６)、届けのあった電子マネーカードＩＤの電子マネーカード１０にＳＯＳデータ１６０を発信させるために、図１５に示すＳＯＳ発信指示データ８０を人工衛星２５へ送信し(ステップ３６１７)、その後、人工衛星２５との間のセッションを解放する(ステップ３６１８)。次に、届けのあった電子マネーカードＩＤの電子マネーカード１０の発行金融機関２６との間でセッションを開設し(ステップ３６１９)、届けのあった電子マネーカードＩＤの電子マネーカード１０の紛失盗難を連絡し(ステップ３６２０)、連絡し終ったら発行金融機関２６との間のセッションを解放し(ステップ３６２１)、その後、終了すなわち緊急受付装置２３からの呼出信号受信待ち状態となる。

【０２４４】次に、ＳＯＳ１２０の届けである場合は(ステップ３６２２)、届けのあった電子マネーカードＩＤの電子マネーカード１０にＳＯＳデータ１６０の発信を停止させるために、図１７に示すＳＯＳ停止指示データ１００を人工衛星２５へ送信し(ステップ３６２３)、その後、人工衛星２５との間のセッションを解放する(ステップ３６２４)。次に、届けのあった電子マネーカードＩＤの電子マネーカード１０の発行金融機関２６との間でセッションを開設し(ステップ３６２５)、紛失盗難のあった電子マネーカードＩＤの電子マネーカード１０が保有していた電子マネーおよびその他データを発行金融機関２６へ送信し(ステップ３６２６)、送信し終ったら発行金融機関２６との間のセッションを解放し(ステップ３６２７)、その後、終了すなわち緊急受付装置２３からの呼出信号受信待ち状態となる。

【０２４５】図３８は、人工衛星２５の動作を示すフローチャートである。

【０２４６】人工衛星２５の動作においては、事象待ち状態で待機しており、この待ち状態が解除されたときに動作を開始する。そして、どの事象が発生したのかの切分けが行なわれる。この切分けによって、
①紛失盗難センタ２４からの呼出し(ステップ３８０１)、
②タイマのタイムアウト(ステップ３８０２，３８０３)
の発生事象が判明する。

【０２４７】以降、この発生事象ごとに個別に説明していく。

【０２４８】まず、紛失盗難センタ２４からの呼出しの場合は(ステップ３８０１)、紛失盗難センタ２４との間でセションを開設し(ステップ３８０４)、紛失盗難センタ２４からデータを受信し(ステップ３８０５)、受信し終ったら紛失盗難センタ２４とのセションを解放する(ステップ３８０６)。その後、紛失盗難センタ２４から受信したデータが図１５に示すＳＯＳ発信指示データ８０か否かをチェックする(ステップ３８０７)。ＳＯＳ発信指示データ８０であれば、図１６に示すＳＯＳ発信指示ブロードキャストデータ９０をブロードキャストする(ステップ３８０８)。その後、タイマＴ１２をセットし(ステップ３８０９)、終了すなわち紛失盗難センタ２４からの呼出待ち状態となる。

【０２４９】ステップ３８０７でのチェックの結果、受信したデータがＳＯＳ発信指示データ８０でない場合、すなわち図１７に示すＳＯＳ停止指示データ１００である場合は、図１１に示すＳＯＳ停止指示ブロードキャスト１１０をブロードキャストする(ステップ３８１０)。その後、タイマＴ１３をセットし(ステップ３８１１)、終了すなわち紛失盗難センタ２４からの呼出待ち状態となる。

【０２５０】次に、タイムアウトは、
①ＳＯＳ発信指示ブロードキャストデータ９０をブロードキャストするためのタイムアウト、
②ＳＯＳ停止指示ブロードキャスト１５０をブロードキャストするためのタイムアウト、
に分類される。

【０２５１】以降、このタイムアウトごとに個別に説明していく。

【０２５２】まず、ＳＯＳ発信指示ブロードキャストデータ９０をブロードキャストするためのタイマＴ１２のタイムアウトの場合は(ステップ３８０２)、ＳＯＳ発信

指示ブロードキャストデータ９０をブロードキャストする(ステップ３８１２)。その後、タイマＴ１２をセットし(ステップ３８１３)、終了すなわち紛失盗難センタ２４からの呼出待ち状態となる。

【０２５３】次に、ＳＯＳ停止指示ブロードキャストデータ１５０をブロードキャストするためのタイマＴ１３のタイムアウトの場合は(ステップ３８０３)、ＳＯＳ停止指示ブロードキャストデータ１５０をブロードキャストする(ステップ３８１４)。その後、タイマＴ１３をセットし(ステップ３８１５)、終了すなわち紛失盗難センタ２４からの呼出待ち状態となる。

【０２５４】なお、人工衛星２５を利用する代わりに、ＰＨＳ電話網の基地局、あるいはテレビジョン信号の垂直帰線期間などの空き時間を利用し、ＳＯＳ発信指示等を行うようにしてもよい。

【０２５５】

【発明の効果】以上の説明から明らかなように、本発明によれば、紛失や盗難にあった電子通貨取引機あるいは電子通貨取引機に収納されている電子化通貨やその他のデータを容易に回収することができる。

【０２５６】また、電子通貨取引機の身体からの落下や使用後の置忘れによる紛失を防止することができる。

【０２５７】さらに、規定時間を経過するごとに電子通貨取引機の機能を一旦停止し、同規定時間ごとに変更されるパスワードの入力によって電子通貨取引機の機能停止を解除していめため、電子通貨取引機の安全性を高めることができるようになる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すシステム構成図である。

【図２】電子通貨取引機の操作面側構成を示す図である。

【図３】電子通貨取引機の内部構成を示すブロック図である。

【図４】電子通貨取引機とＰＯＳとの間で取引を行う場合の処理の概要を示す図である。

【図５】紛失盗難防止機能の主要部の構成を示すシステム構成図である。

【図６】カウンタパーツの構成を示す機能ブロックである。

【図７】２４時間有効パスワードの例１を示す図である。

【図８】２４時間有効パスワードの例２を示す図である。

【図９】存在確認問合せデータ(カウンタパーツ→電子マネーカード)の構成図である。

【図１０】問合せによる存在確認応答データ(電子マネーカード→カウンタパーツ)の構成図である。

【図１１】機能再開データ(カウンタパーツ→電子マネーカード)の構成図である。

【図１２】問合せによらない存在確認自発発信データ(電子マネーカード→カウンタパーツ)の構成図である。

【図１３】機能停止データ(カウンタパーツ→電子マネーカード)の構成図である。

【図１４】取引機能停止の内容を示す説明図である。

【図１５】ＳＯＳ発信指示データ(紛失盗難センタ→人工衛星)の構成図である。

【図１６】ＳＯＳ発信指示ブロードキャストデータ(人工衛星→電子マネーカード)の構成図である。

【図１７】ＳＯＳ停止指示データ(紛失盗難センタ→人工衛星)の構成図である。

【図１８】ＳＯＳ停止指示兼ＳＯＳ廃棄指示データ(人工衛星→電子マネーカード)の構成図である。

【図１９】ＳＯＳデータ(電子マネーカード→電子マネーカード)の構成図である。

【図２０】緊急パーツのデータ内容を示す構成図である。

【図２１】電子マネーカードの紛失盗難防止に関わる基本動作を示すフローチャートである。

【図２２】緊急受付装置との取引処理を示すフローチャートである。

【図２３】他機／自機内取引処理を示すフローチャートである。

【図２４】衝撃検出対応処理を示すフローチャートである。

【図２５】自カードＩＤ受信時の処理を示すフローチャートである。

【図２６】図２５の続きを示すフローチャートである。

【図２７】他カードＩＤ受信時の処理を示すフローチャートである。

【図２８】タイムアウト処理を示すフローチャートである。

【図２９】図２８の続きを示すフローチャートである。

【図３０】共通処理を示すフローチャートである。

【図３１】図３０の続きを示すフローチャートである。

【図３２】カウンタパーツの動作を示すフローチャートである。

【図３３】図３２の続きを示すフローチャートである。

【図３４】図３３の続きを示すフローチャートである。

【図３５】緊急受付装置の動作を示すフローチャートである。

【図３６】紛失盗難センタの動作を示すフローチャートである。

【図３７】図３６の続きを示すフローチャートである。

【図３８】人工衛星の動作を示すフローチャートである。

【符号の説明】

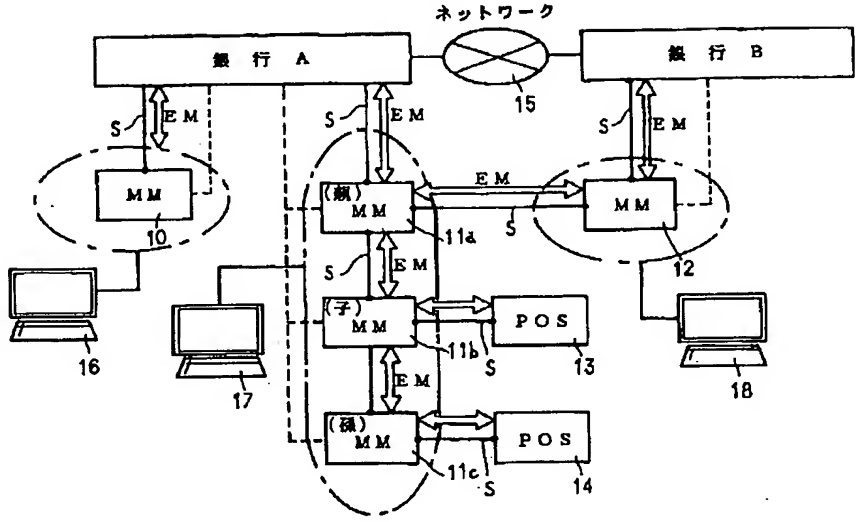
１０，１１ａ～１１ｃ，１２…電子通貨取引機、１３，１４…ＰＯＳ端末、１５…ネットワーク、１４３，１４４，１４５…送受信機、１４６…ＧＰＳ、２１…カウン

35　　36

タパーツ、２２…緊急パーツ、２３…緊急受付装置、２＊　＊４…紛失盗難センタ、２５…人工衛星。

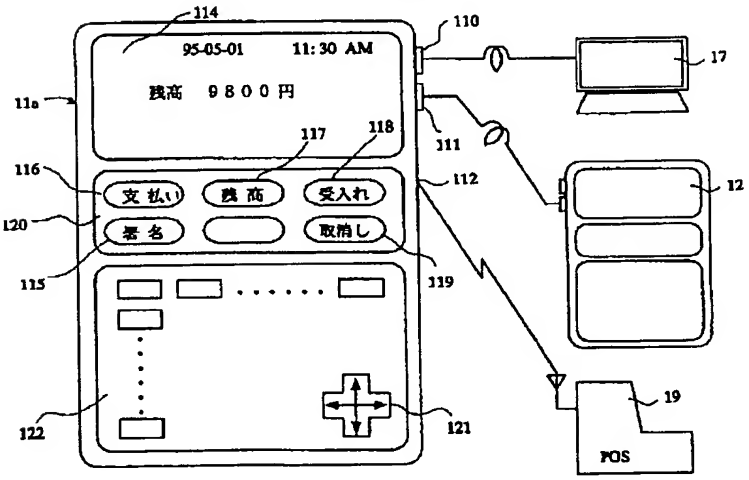
【図１】

図１



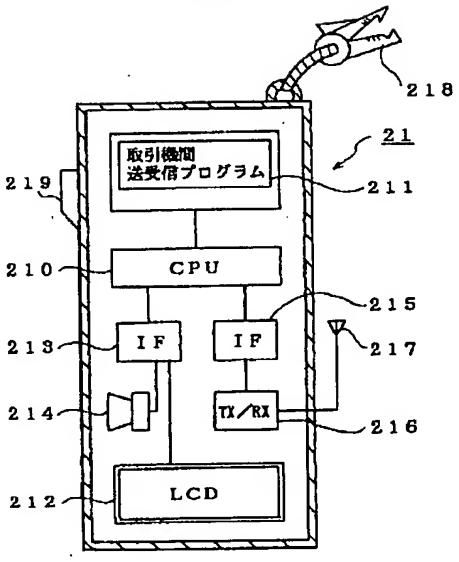
【図２】

図２



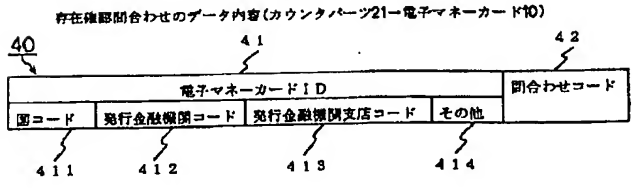
【図６】

図６



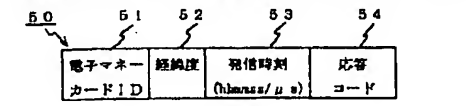
【図９】

図９



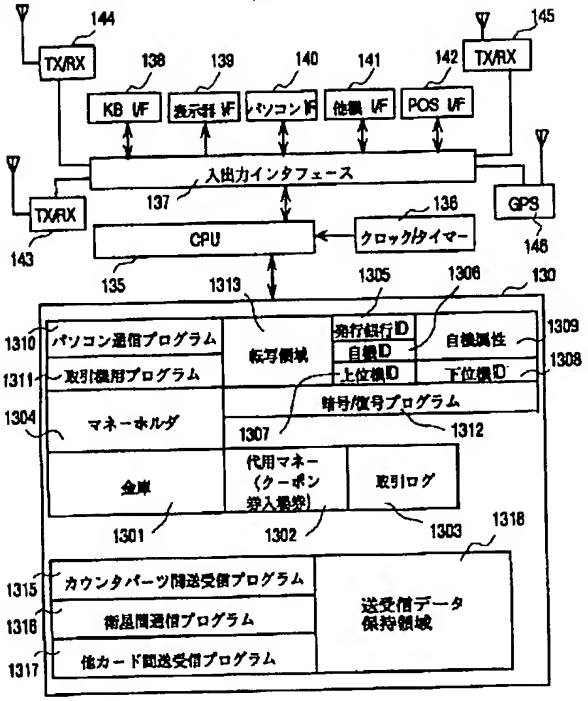
【図１０】

図１０



【図３】

図３



【図７】

図７

２４Ｈ有効パスワード例１

真偽混合パスワード	曜日	パスワード入力数	
		真(パスワードは任意)	偽(パスワードは任意)
Pt1	日	1	3
:	月	2	2
Ptn	火	3	1
Pf1	水	4	0
:	木	3	1
:	金	2	2
Pfm	土	1	3

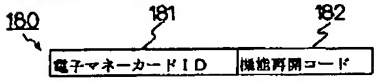
Pt1～Ptn：真パスワード

Pf1～Pfm：偽パスワード

【図１１】

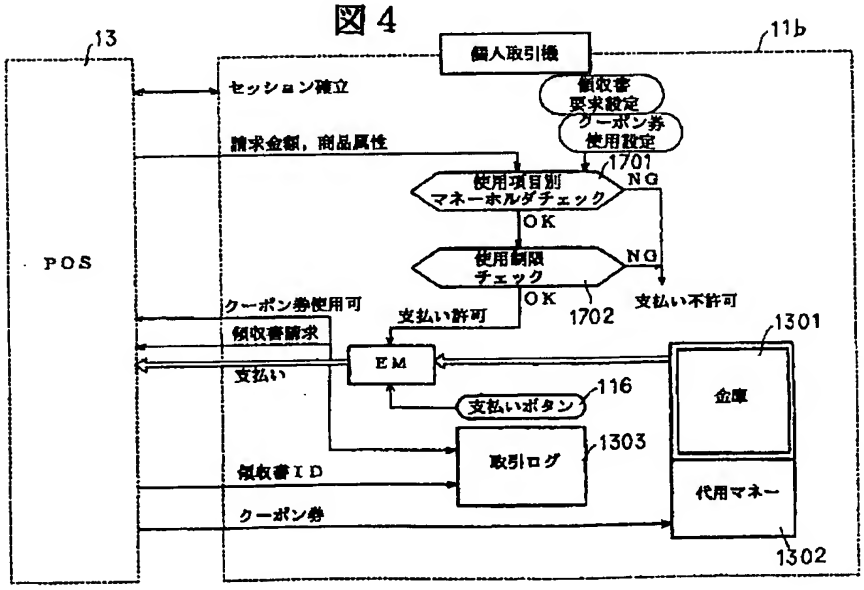
図１１

機能再開のデータ内容(カウンタパーツ21ー電子マネーカード10)



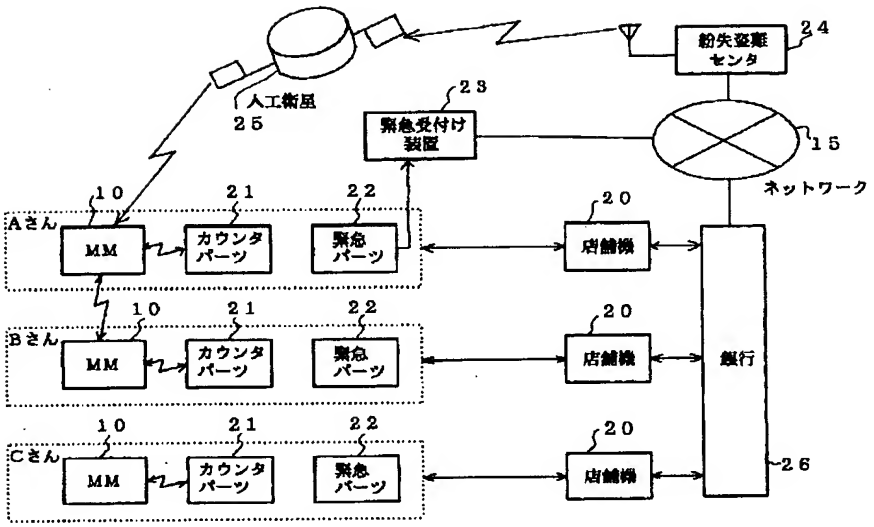
【図４】

図４



【図５】

図５



【図８】

図８

２４Ｈ有効パスワード例２

真偽混合パスワード	Bにち下１桁	パスワード入力数 真(パスワードは任意)	パスワード入力数 偽(パスワードは任意)
Pt1	0	5	0
:	1	4	1
:	2	3	2
:	3	2	3
Ptn	4	1	4
Pf1	5	5	0
:	6	4	1
:	7	3	2
:	8	2	3
Pfm	9	1	4

Pt1～Ptn：真パスワード
Pf1～Pfm：偽パスワード

【図１２】

図１２

存在確認自発発信のデータ内容(電子マネーカードID→カウンタパーツ21)

60	61	62	63	64
	電子マネーカードＩＤ	経緯度	発信時刻 (hhmmss/μs)	自発発信コード

【図１３】

図１３

機能停止のデータ内容(カウンタパーツ21→電子マネーカードID)

70	71	72	73
	電子マネーカードＩＤ	機能停止時間 hhmm	機能停止コード

【図１４】

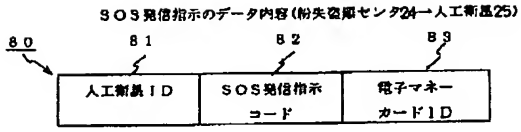
図１４

取引機能停止の内容

	取引内容	第１級	第２級	第３級
	緊急受付け装置との取引	○	○	○
	店舗用取引装置との取引 (緊急受付け装置の代行)	×	○	○
	パスワード入力	×	×	○

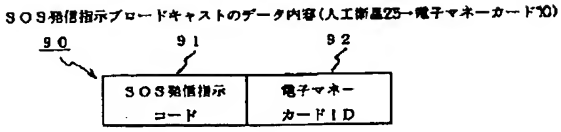
【図１５】

図１５



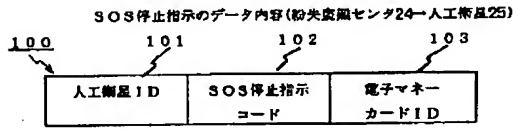
【図１６】

図１６



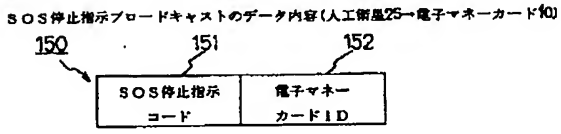
【図１７】

図１７



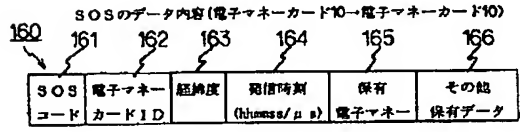
【図１８】

図１８



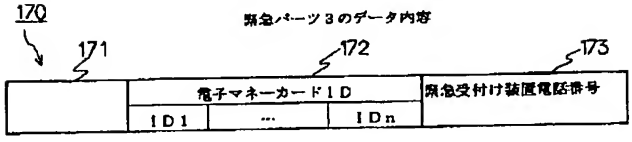
【図１９】

図１９



【図２０】

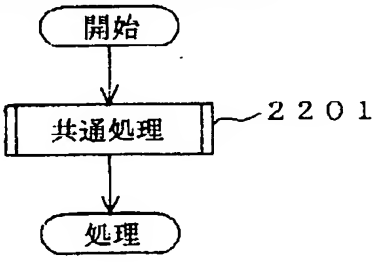
図２０



【図２２】

図２２

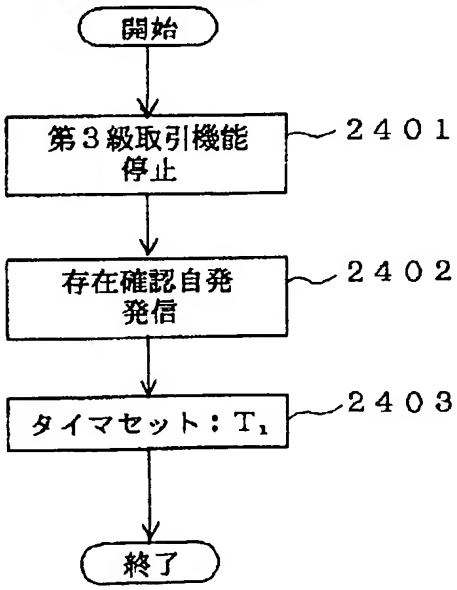
緊急受付装置との取引処理



【図２４】

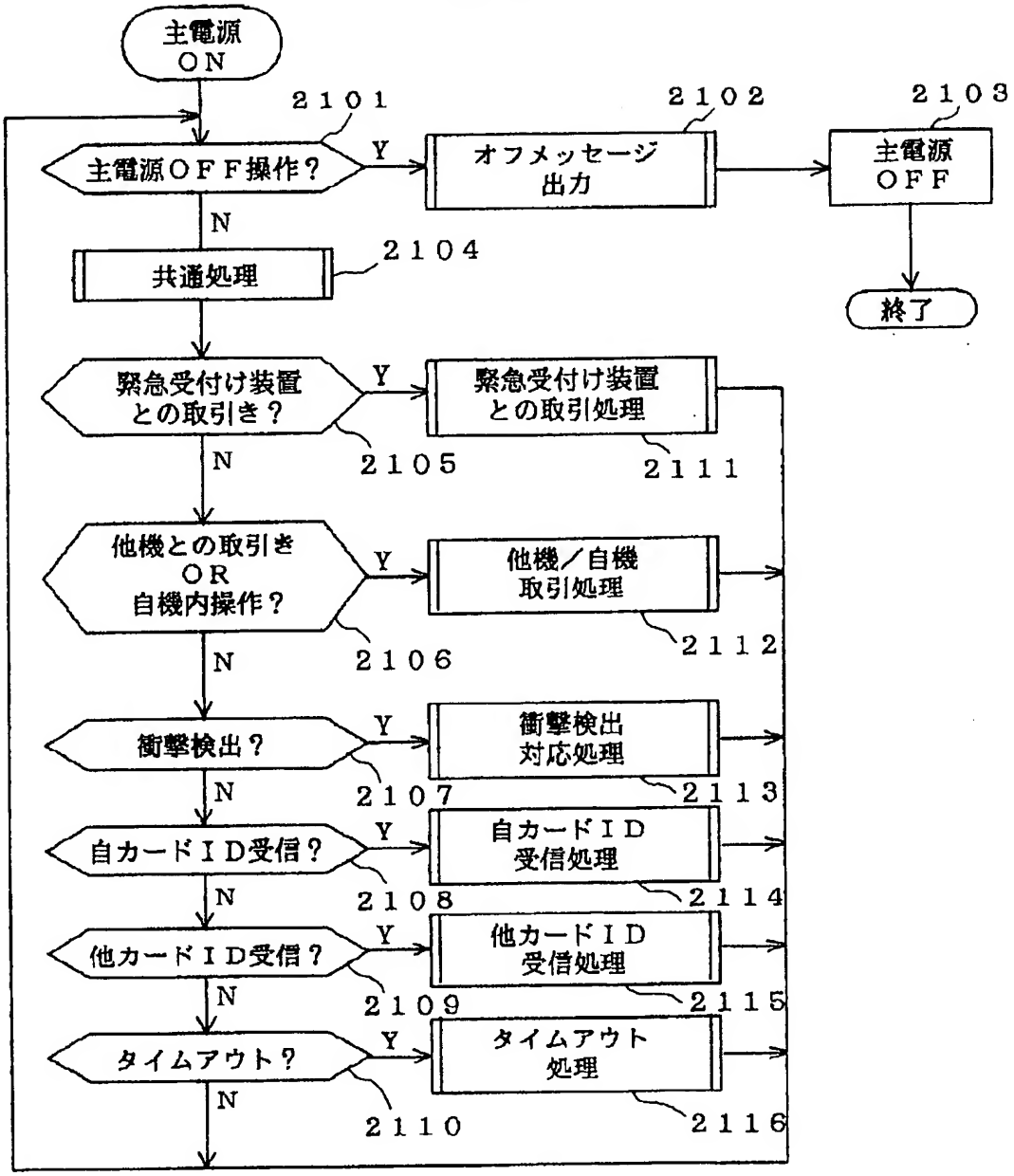
図２４

衝撃検出対応処理



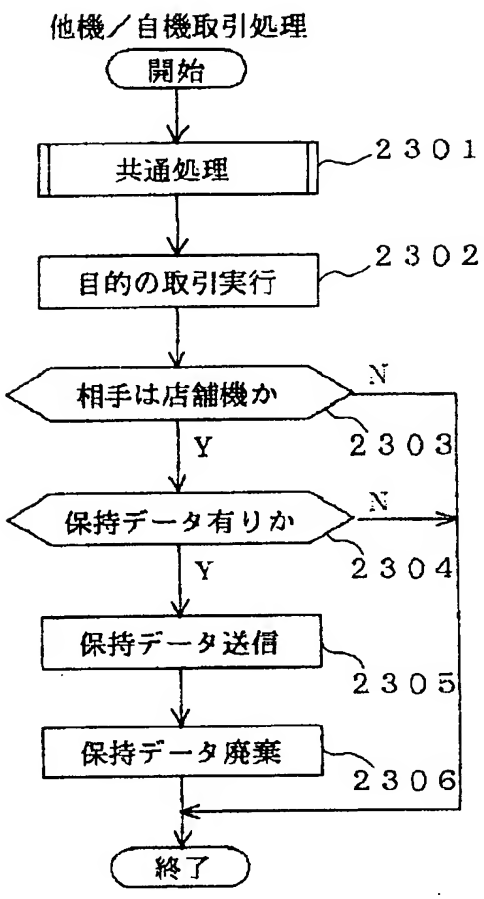
【図２１】

図２１


主電源
ＯＮ
２１０１
主電源ＯＦＦ操作？
Y
２１０２
オフメッセージ
出力
２１０３
主電源
ＯＦＦ
終了
N
２１０４
共通処理
緊急受付け装置
との取引き？
Y
２１０５
緊急受付け装置
との取引処理
２１１１
N
他機との取引き
ＯＲ
自機内操作？
Y
２１０６
他機／自機
取引処理
２１１２
N
衝撃検出？
Y
２１０７
衝撃検出
対応処理
２１１３
N
自カードＩＤ受信？
Y
２１０８
自カードＩＤ
受信処理
２１１４
N
他カードＩＤ受信？
Y
２１０９
他カードＩＤ
受信処理
２１１５
N
タイムアウト？
Y
２１１０
タイムアウト
処理
２１１６
N

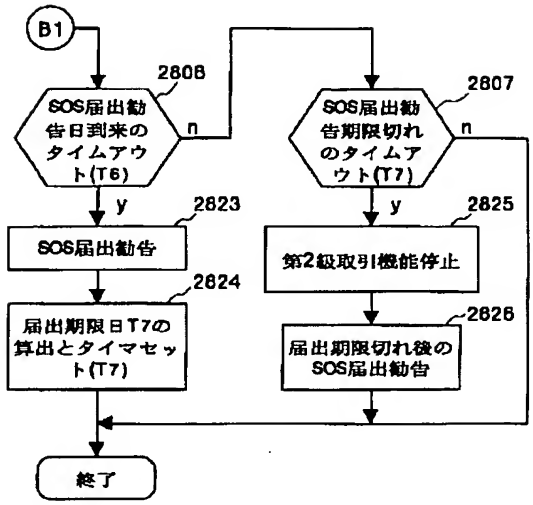
【図２３】

図２３



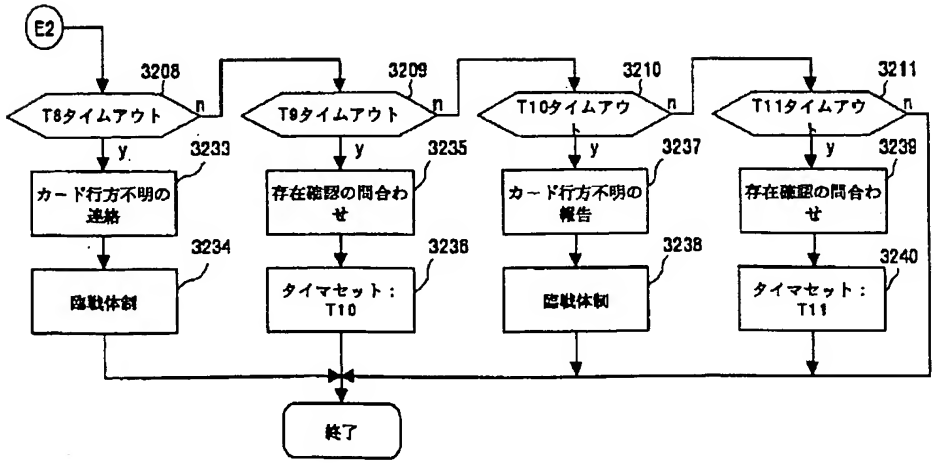
【図２９】

図２９



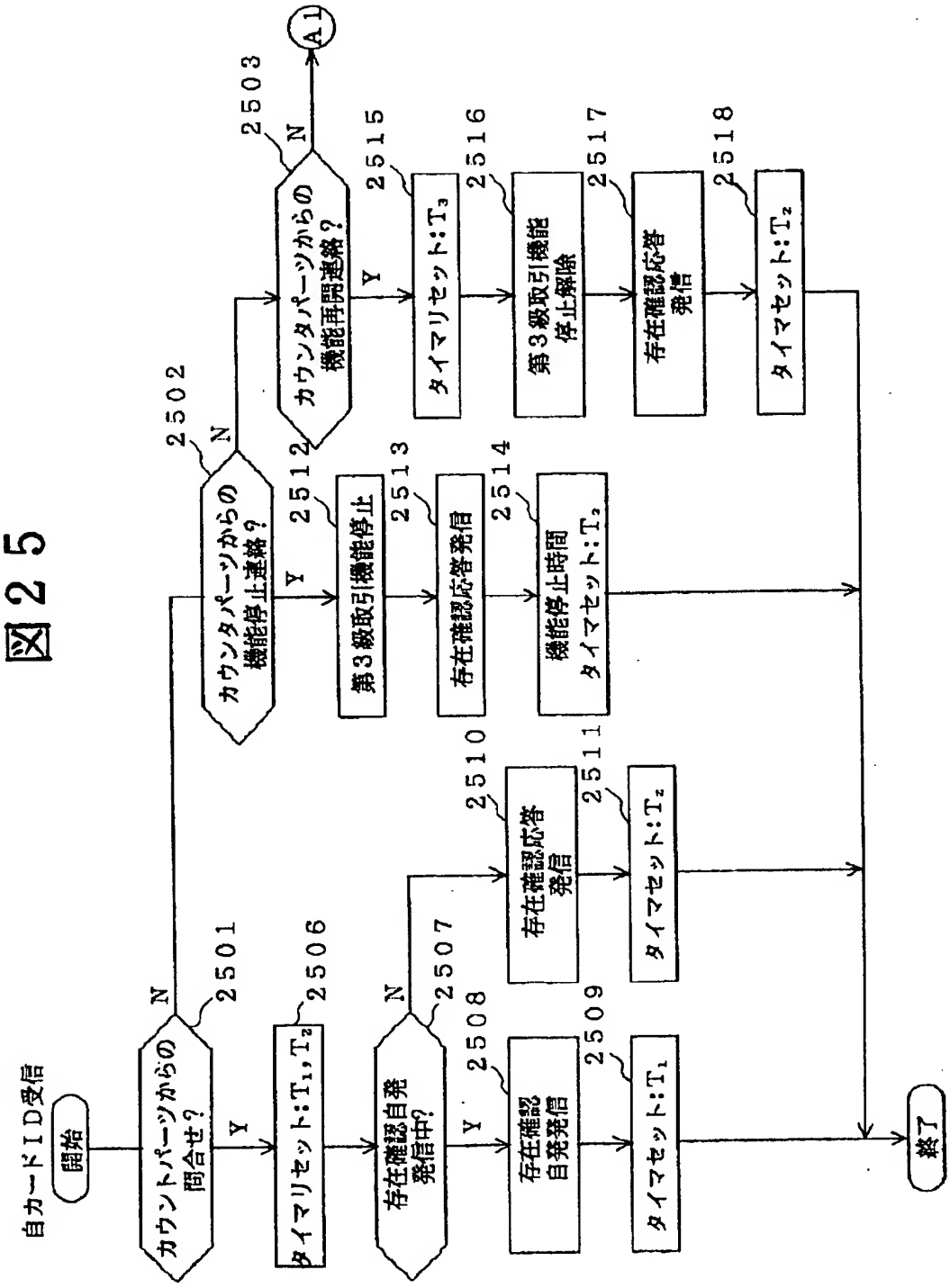
【図３４】

図３４



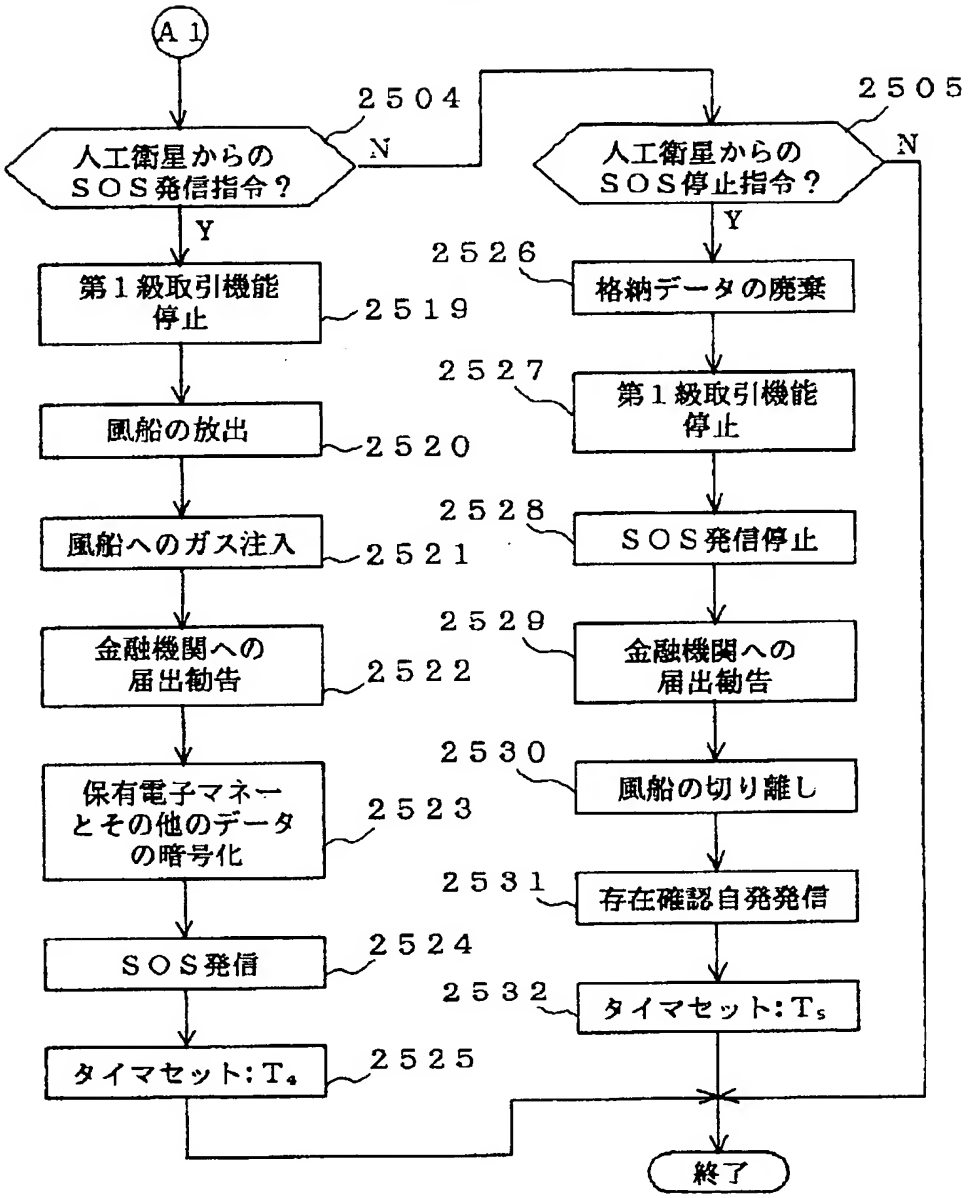
【図２５】

図２５


自カードＩＤ受信
開始
カウントパーツからの問合せ?
2501
N
Y
タイマリセット:T1,T2
2506
存在確認自発発信中?
2507
N
Y
存在確認自発発信
2508
タイマセット:T1
2509
カウンタパーツからの機能停止連絡?
2502
N
Y
第３級取引機能停止
2512
存在確認応答発信
2513
機能停止時間タイマセット:T2
2514
存在確認応答発信
2510
タイマセット:T2
2511
カウンタパーツからの機能再開連絡?
2503
N
Y
A1
タイマリセット:T3
2515
第３級取引機能停止解除
2516
存在確認応答発信
2517
タイマセット:T2
2518
終了

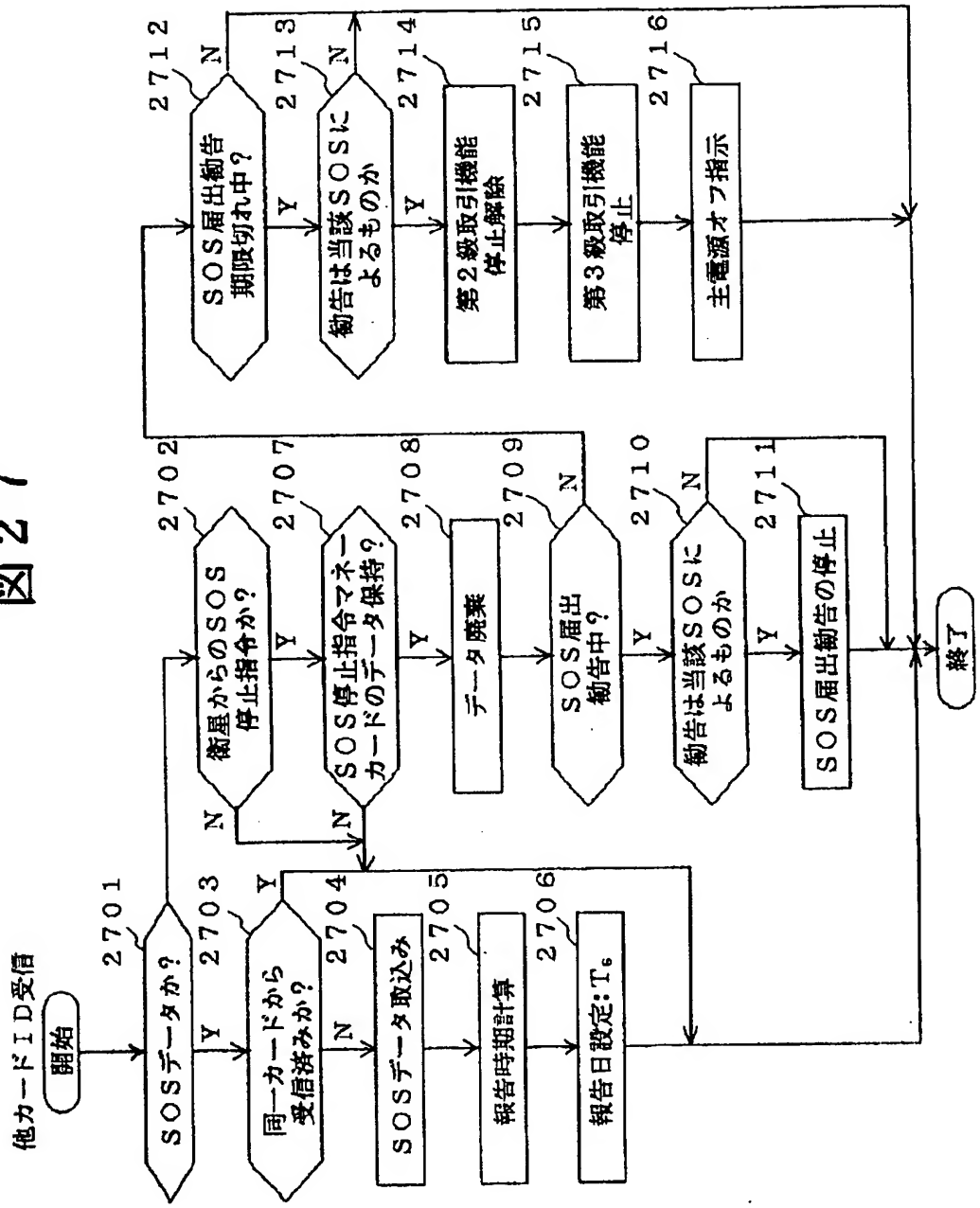
【図２６】

図２６


A 1
2504
人工衛星からの
ＳＯＳ発信指令？
N
Y
2505
人工衛星からの
ＳＯＳ停止指令？
N
Y
第１級取引機能
停止
2519
風船の放出
2520
風船へのガス注入
2521
金融機関への
届出勧告
2522
保有電子マネー
とその他のデータ
の暗号化
2523
ＳＯＳ発信
2524
タイマセット：Ts
2525
2526
格納データの廃棄
2527
第１級取引機能
停止
2528
ＳＯＳ発信停止
2529
金融機関への
届出勧告
2530
風船の切り離し
2531
存在確認自発発信
2532
タイマセット：Ts
終了

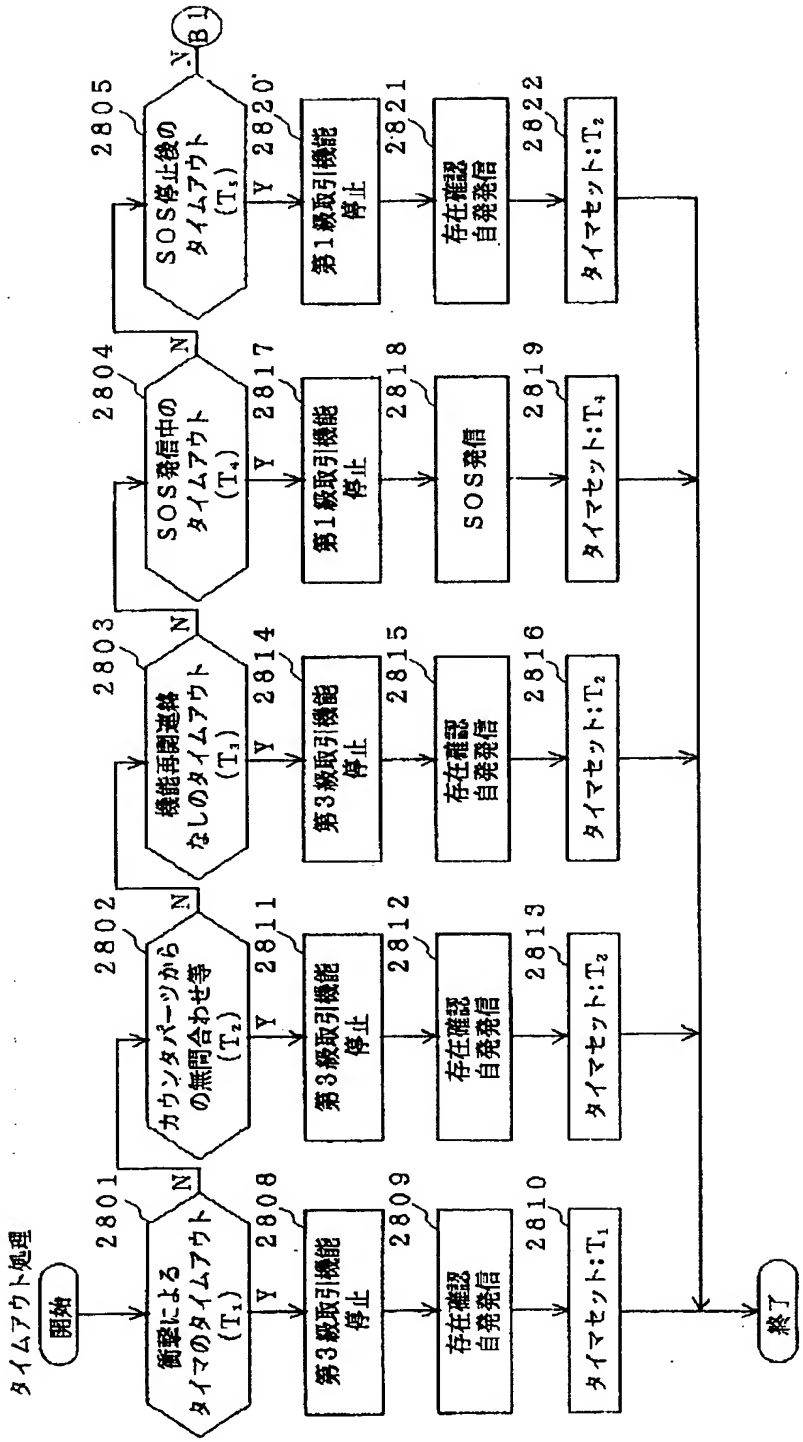
【図２７】

図２７


他カードＩＤ受信
開始
２７０１
ＳＯＳデータか？
Ｙ
２７０３
同一カードから受信済みか？
Ｎ
２７０４
ＳＯＳデータ取込み
２７０５
報告時期計算
２７０６
報告日設定：Ｔ６
Ｙ
２７０２
衛星からのＳＯＳ停止指令か？
Ｎ
２７０７
ＳＯＳ停止指令マネーカードのデータ保持？
Ｎ
２７０８
データ廃棄
２７０９
ＳＯＳ届出勧告中？
Ｎ
２７１０
勧告は当該ＳＯＳによるものか
Ｙ
２７１１
ＳＯＳ届出勧告の停止
２７１２
ＳＯＳ届出勧告期限切れ中？
Ｎ
２７１３
勧告は当該ＳＯＳによるものか
Ｙ
２７１４
第２級取引機能停止解除
２７１５
第３級取引機能停止
２７１６
主電源オフ指示
終了

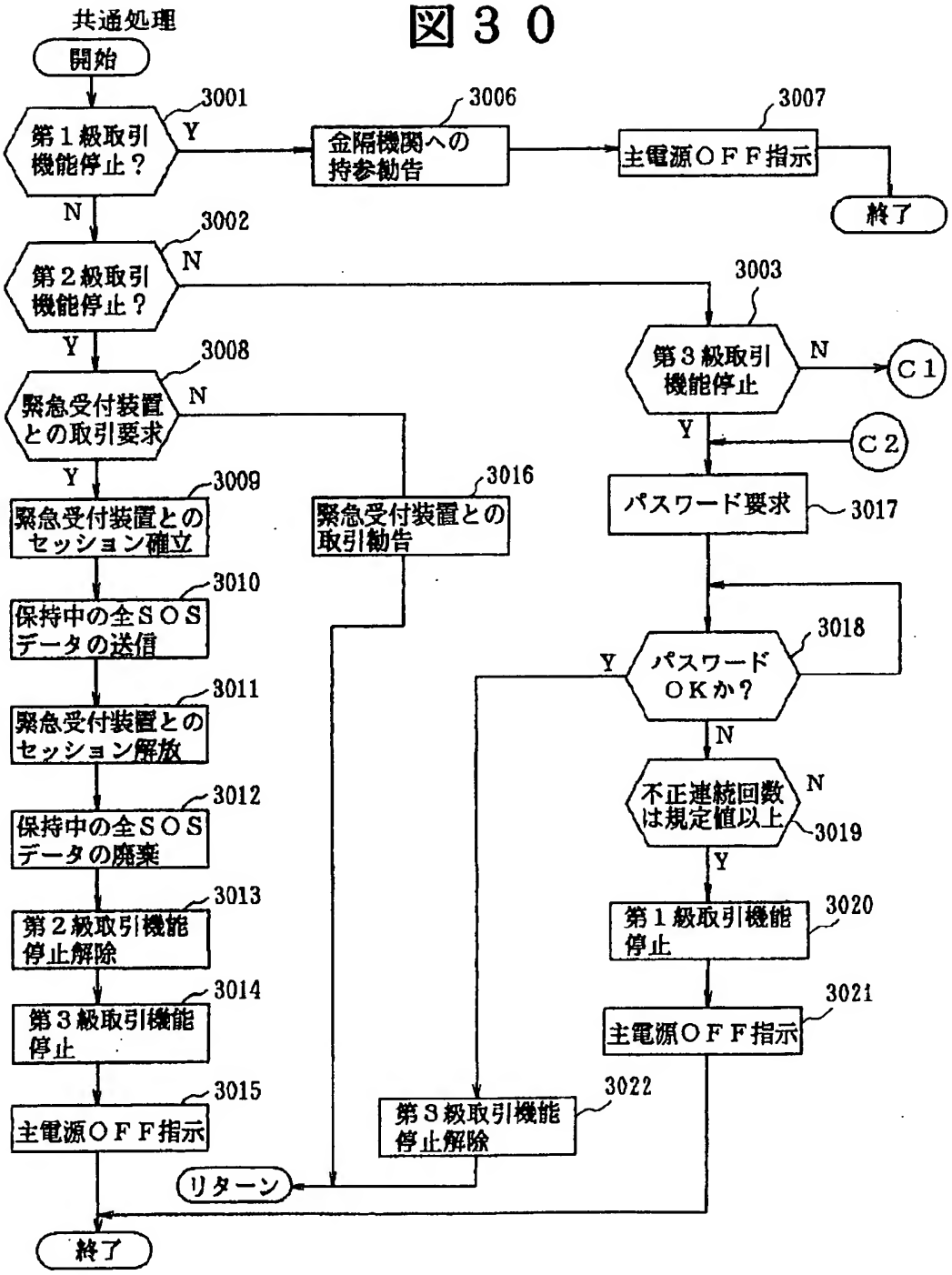
【図２８】

図２８


タイムアウト処理
開始
2801
衝撃によるタイマのタイムアウト (T1)
Y
N
2808
第3級取引機能停止
2809
存在確認自発発信
2810
タイマセット:T1
2802
カウンタパーツからの無問合わせ等 (T2)
2811
第3級取引機能停止
2812
存在確認自発発信
2813
タイマセット:T2
2803
機能再開連絡なしのタイムアウト (T3)
2814
第3級取引機能停止
2815
存在確認自発発信
2816
タイマセット:T2
2804
SOS発信中のタイムアウト (T4)
2817
第1級取引機能停止
2818
SOS発信
2819
タイマセット:T4
2805
SOS停止後のタイムアウト (T5)
2820
第1級取引機能停止
2821
存在確認自発発信
2822
タイマセット:T2
B1
終了

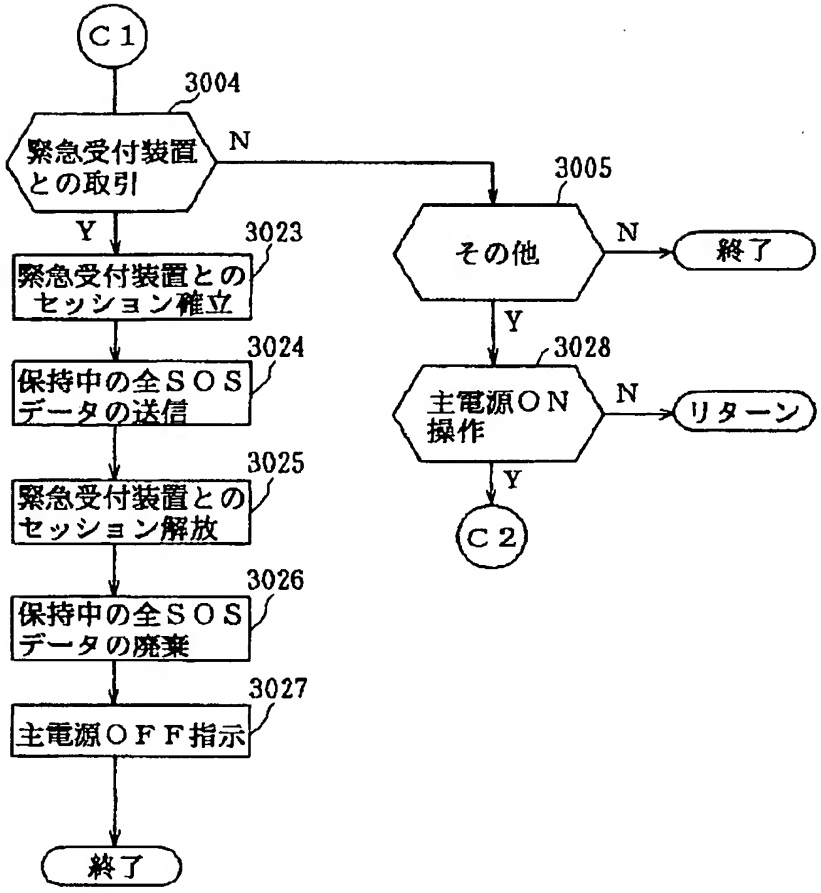
【図３０】

図３０


共通処理
開始
3001
第１級取引機能停止？
Y
3006
金隔機関への持参勧告
3007
主電源ＯＦＦ指示
終了
N
3002
第２級取引機能停止？
N
3003
第３級取引機能停止
N
C1
Y
C2
Y
3008
緊急受付装置との取引要求
N
Y
3009
緊急受付装置とのセッション確立
3016
緊急受付装置との取引勧告
パスワード要求
3017
3010
保持中の全ＳＯＳデータの送信
3018
パスワードＯＫか？
Y
3011
緊急受付装置とのセッション解放
N
3012
保持中の全ＳＯＳデータの廃棄
不正連続回数は規定値以上
N
3019
Y
3013
第２級取引機能停止解除
第１級取引機能停止
3020
3014
第３級取引機能停止
主電源ＯＦＦ指示
3021
3015
主電源ＯＦＦ指示
第３級取引機能停止解除
3022
リターン
終了

【図３１】

図３１


Ｃ１
3004
緊急受付装置との取引
N
Y
3023
緊急受付装置とのセッション確立
3024
保持中の全ＳＯＳデータの送信
3025
緊急受付装置とのセッション解放
3026
保持中の全ＳＯＳデータの廃棄
3027
主電源ＯＦＦ指示
終了
3005
その他
N
終了
Y
3028
主電源ＯＮ操作
N
リターン
Y
Ｃ２

【図３２】

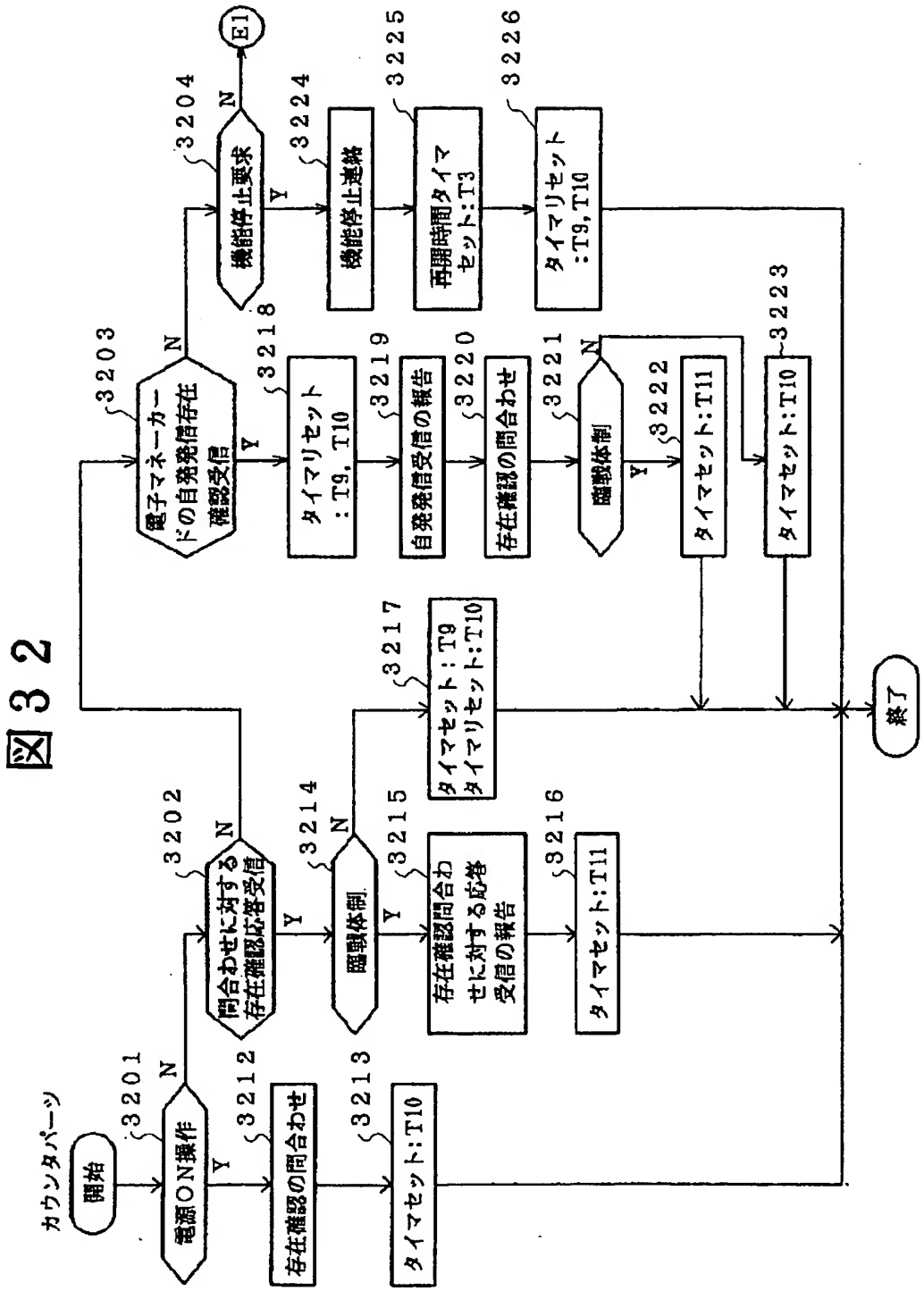
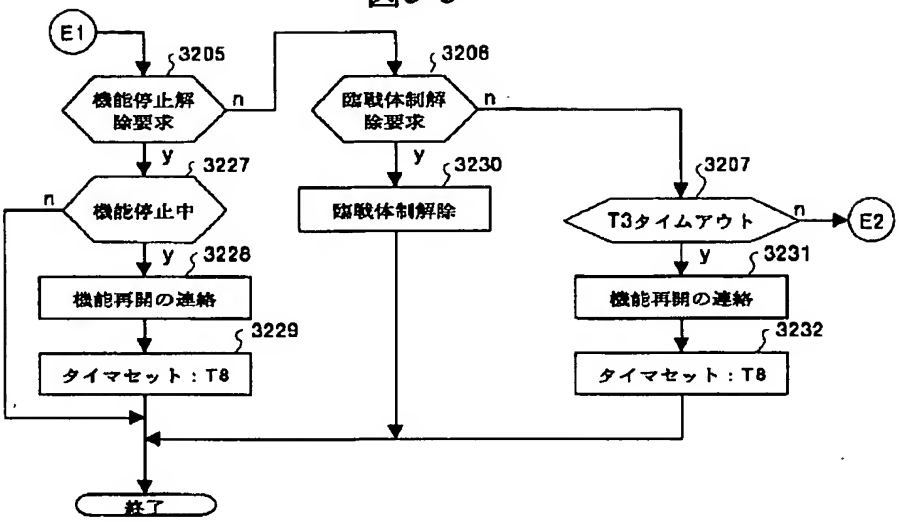


図３２
カウンタパーツ
開始
電源ON操作
3201
N
Y
存在確認の問合わせ
3212
タイマセット:T10
3213
問合わせに対する存在確認応答受信
3202
N
Y
3214
N
Y
3215
存在確認問合わせに対する応答受信の報告
3216
タイマセット:T11
タイマセット:T9
タイマリセット:T10
3217
電子マネーカードの自発発信存在確認受信
3203
N
Y
3218
タイマリセット:T9, T10
3219
自発発信受信の報告
3220
存在確認の問合わせ
3221
N
Y
3222
タイマセット:T11
3223
タイマセット:T10
機能停止要求
3204
N
Y
E1
3224
機能停止連絡
3225
再開時間タイマセット:T3
3226
タイマリセット:T9, T10
終了

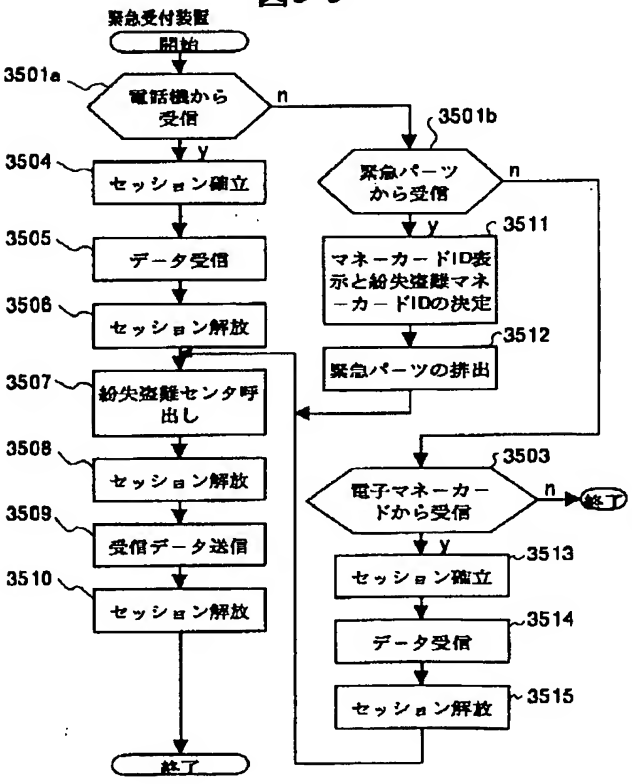
【図３３】

図3 3



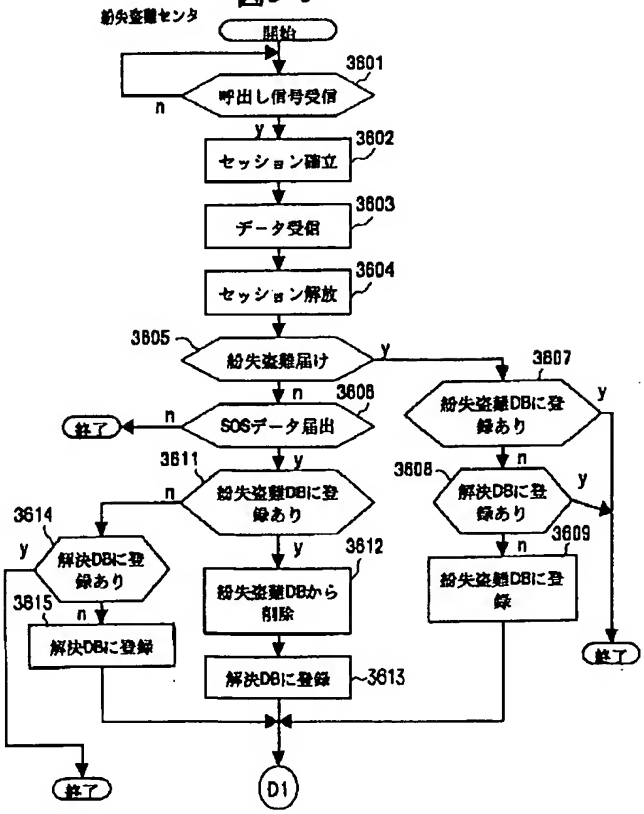
【図３５】

図3 5



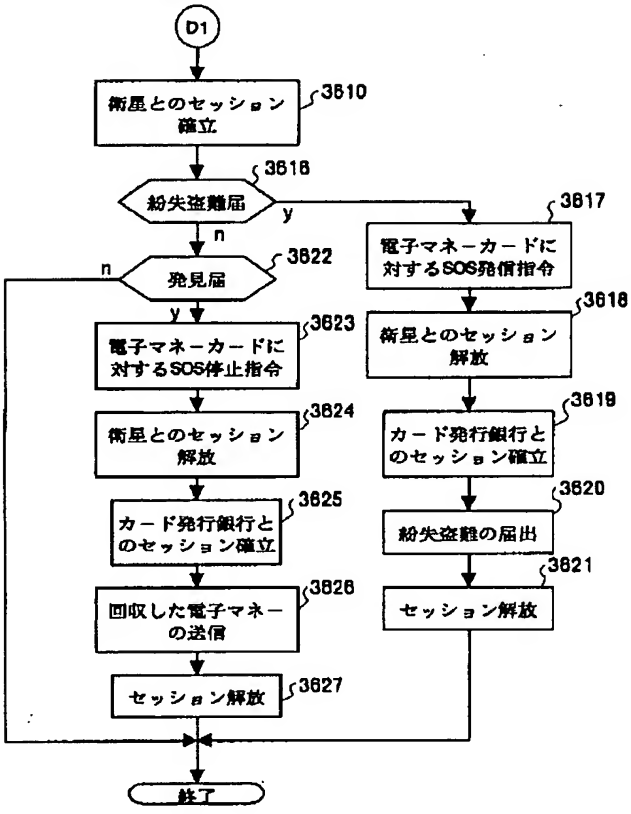
【図３６】

図3 6



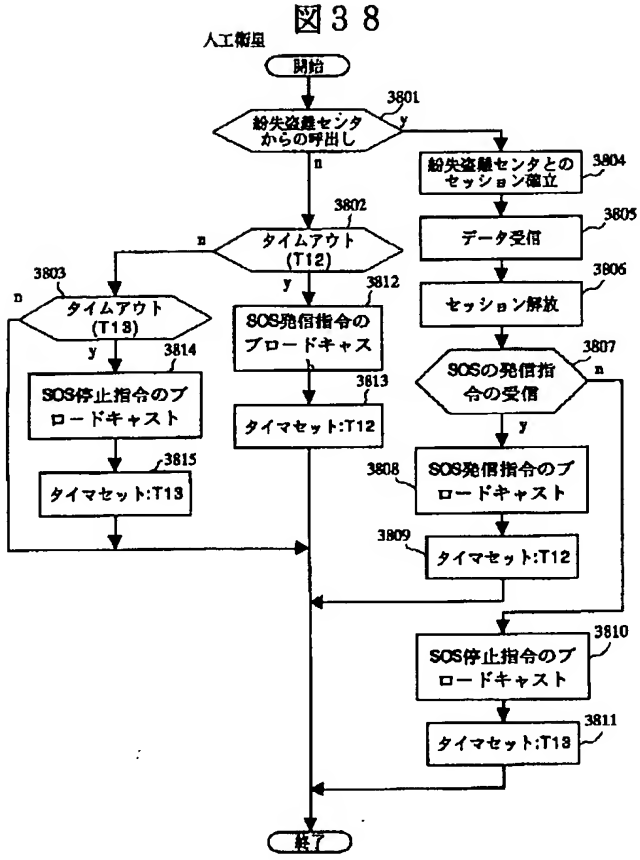
【図３７】

図３７



【図３８】

図３８



フロントページの続き

(51)Int.Cl.[6]　　識別記号　　ＦＩ

Ｈ０４Ｌ　9/32　　Ｈ０４Ｂ　7/26　　１０９Ｒ

Ｈ０４Ｌ　9/00　　６７３Ｂ

(72)発明者　山田　英雄
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　瀧本　勇一
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内